La privacidad en las ciudades inteligentes

Privacy in Smart cities

Rubén Enrique Rodríguez Samudio[1]

Fecha correspondencia:
Recibido: 15 de septiembre de 2019.
Revisión: 27 de septiembre de 2019.
Aceptado: 17 de octubre de 2019.

Forma de citar:
Rodríguez, Rubén Enrique. La privacidad en las ciudades inteligentes. Revista CES Derecho. Vol. 10, No. 2, julio –diciembre de 2019, 675-695.

Open access
Términos de uso
Licencia creative commons
Ética de publicaciones
Revisión por pares
Gestión por Open Journal System
DOI: http://dx.doi.org/10.21615/cesder.10.2.7
ISSN: 2145-7719

Sobre los autores:

1. Investigador, Universidad de Hokkaido, Japón. Profesor Adjunto, Universidad de Keio, Japón. Doctor en derecho, Universidad de Hokkaido, Japón.

Resumen

El concepto original de la privacidad como derecho, introducido a finales del siglo XIX, hacia énfasis en el derecho del individuo en no ser molestado. Desde entonces, cada nuevo desarrollo tecnológico ha contribuido a un cambio fundamental en el concepto de la privacidad. El uso de tecnologías digitales se tradujo en nacimiento de la idea de control de datos. La introducción de tecnologías de la información a nivel de uso doméstico, como lo son tecnologías del internet de las cosas, aunados a nuevos sistemas de procesamiento de datos mediante algoritmos de macro datos y computación en la nube suponen un cambio de paradigma en la sociedad moderna. Las ciudades inteligentes en donde los servicios públicos y privados hacen uso de la información personal de los ciudadanos, hacen necesario nuevamente un replanteamiento del concepto de privacidad.

Palabras clave: Privacidad, Ciudades Inteligentes, Internet de las Cosas, Macro Datos, Computación en la Nube.

Abstract

The original concept of privacy as a right, introduced during the late 19th century, was centered on the right to be left alone. Since then, each new technological development has contributed to a fundamental change in the concept of privacy. The use of digital technologies brought forth the concept of data control. The introduction of information technologies at domestic level, such as the Internet of Things, paired with new data processing methods via algorithms using Big Data or Cloud Computing entail a paradigm shift in modern society. Smart Cities, where public and private services make use of their citizens´ personal information, require a new approach to the concept of privacy.

Keywords: Privacy, Smart Cities, Internet of Things, Big Data, Cloud Computing.

Introducción

Este artículo discute los retos de un derecho a la protección de datos en un mundo donde la interconectividad y la acumulación de información son cada vez más necesarios para el desenvolvimiento social. El orden social de una comunidad se ve vinculado a su desarrollo tecnológico. Desde el descubrimiento de técnicas de cultivo que permitieron el desarrollo de las civilizaciones antiguas, hasta los avances producto de la revolución industrial que dieron lugar a la producción en gran escala de productos y el surgimiento de nuevas industrias de servicios. Entrado el siglo XX este desarrollo

se enfocó no en una revolución energética, sino de tecnologías de información, al punto que la sociedad moderna ha sido diseñada, y está siendo desarrollada, en base a la información.

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. La implementación de tecnologías de la información en la vida diaria de individuos y comunidades ha sido objeto de estudio de varias instituciones gubernamentales. La Comisión Federal de Comercio de los Estados Unidos (FTC, 2015) considera que tecnologías relativas al internet de las cosas se traducirán en beneficios en el sector de la salud, consumo de energía y transporte vial, tanto público y privado. Una perspectiva similar puede encontrarse en la Unión Europea, en particular dentro del contexto del desarrollo de ciudades inteligentes (EC).

En Asia, el gobierno de Japón ha lanzado la iniciativa Construyendo la Sociedad 5.0 (Realizing Society 5.0), definiéndola como una sociedad con el ser humano como su elemento fundamental, la cual se enfoca en el balance entre los avances económicos y la solución de problemas sociales mediante un sistema que integra tanto las estructuras físicas como el ciber espacio (Science and Technology Policy. Council for Science, Technology and Innovation, s.f.).

Sin embargo, la integración de estas tecnologías también conlleva el surgimiento de nuevos riesgos en materia de recolección, protección y uso de datos personales. Aunado a esto, los sistemas tradicionales de protección de datos personales fundamentados en un derecho a la privacidad bajo el modelo Warren-Brandeis (Warren & Brandeis, 1890) se basan en el concepto de control sobre la publicación. La privacidad, como se concibió en un primer momento, protegía intereses no económicos del individuo siguiendo un modelo *ius privatista* del ejercicio del derecho enfocado a resolver conflictos entre particulares. Este modelo no se adapta al surgimiento de nuevas tecnologías, por lo que, a partir de la década de los años 60 y 70, ha venido siendo remplazado por modelos que hacen énfasis en el control de datos personales en un mundo interconectado.

Dos fenómenos han producido un cambio fundamental en la dinámica de la privacidad. El primero es la escala de la información recolectada. La privacidad, en su sentido originario, fue estructurada para hacer frente a la obtención de información personal en medios análogos, como lo son fotografías o cartas. Aún con la invención de máquinas de fotocopiado, la violación de la privacidad de un individuo se veía limitada a la existencia del objeto físico que contenía la información. Esta limitación física también limitaba la divulgación de la información personal tanto en su contenido como en su alcance. Sin embargo, el desarrollo de tecnologías computacionales durante la segunda guerra mundial resulta en una explosión informática que culmina con la creación de métodos de almacenaje digitales y que actualmente se ha expandido a sistema de almacenaje en la nube.

El segundo fenómeno es la participación de entidades estatales en el esquema de recolección de datos.[1] Originalmente, la privacidad se concibió como una herramienta

1. Un ejemplo claro de esto es la primera ley de protección de datos: la Datalegen sueca. La *Datalegen* no establecía principios generales ni el uso que debía darse los datos personales. En general, la ley simplemente requería un permiso del recién creado Comité de Inspección de Datos para la recolección de datos personales en registros computarizados, principalmente gubernamentales. (Öman, 2004, pág. 390).
Una postura similar puede encontrarse en un informe reporte de 1973 publicado por el Departamento de Salud, Educación y Servicios Sociales de los

para remediar el daño sufrido por un particular producto de la publicación de información privada. Surge como respuesta a las limitaciones inherentes a las leyes de difamación, las cuales no dan daban derecho a una indemnización en caso de que la información fuera cierta. Sin embargo, actualmente es común que actores estatales recolecten información. El caso más extremo puede observarse en el sistema de crédito social de China. El gobierno chino, bajo el argumento de conservar un orden social, ha diseñado un sistema que busca cuantificar el valor social de una persona; el mismo se encuentra a prueba en algunas regiones del país con miras a su implementación total en el año 2020.

Estructuralmente este artículo se divide en tres secciones. La primera examina algunos elementos y la evolución de la teoría clásica de la privacidad. La segunda sección introduce el concepto de ciudades y sociedades inteligentes con enfoque en las tres tecnologías principales que las componen: el internet de las cosas, los macro datos, y los servicios de la nube. La tercera sección se enfoca en tres desafíos de la privacidad en una ciudad inteligente.

I. La doctrina tradicional del derecho a la privacidad

Esta sección sirve como un repaso de las doctrinas tradicionales de privacidad. Desde sus inicios bajo las teorías planteadas por Warren y Brandeis (1890), la privacidad se ha basado en la publicación de información personal sin el previo consentimiento del titular o, como lo acuñaron Warren y Brandeis, el derecho a no ser molestado (*the right to be left alone)* Originalmente, la privacidad se constituía en un derecho eminentemente no patrimonial, y el desarrollo de las doctrinas que velan por su protección surge como resultado del desarrollo de tecnologías fotográficas y las falencias de las doctrinas basadas en la difamación para proteger los intereses de individuos cuya información hubiese sido publicada.

A finales del siglo XIX, cuando el concepto de privacidad comienza a tomar una estructura jurídica determinable. No obstante, la tecnología de la época 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 ende. el rango de información estaba limitada al medio físico donde fuese plasmada. Aunado a esto, la doctrina clásica de la privacidad permite la transferencia del dominio del medio físico donde se encuentre la información, v.gr. la fotografía, pero no su publicación.

En segundo lugar, la naturaleza del daño sufrido en los casos de violación ha cambiado. Bajo la perspectiva clásica, el derecho a la privacidad es un derecho no patrimonial, no adjudicable, por cuanto el daño no puede ser cuantificado materialmente. Esta fue la postura doctrinal hasta la época de los años 50, cuando autores como Nimmer (1954) 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, y 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.

Estados Unidos (U.S. Department of Health, Education & Wellfare, 1973) que reconoce que los particulares deben proporcionar información personal a instituciones sin rostro *(faceless institutions)*, para que la misma sea manejada por individuos desconocidos, y en muchas ocasiones sin que el titular de la información tenga conocimiento siquiera de que la institución guarda un registro sobre sus datos.

La información del individuo, y en particular su recolección y publicación, tienen un valor pecuniario como no pecuniario. Sin embargo, esto implica que definir los límites de la privacidad sea una tarea muy difícil. Como lo expresa Solove (2008), la privacidad es un concepto que abarca, entre otras cosas, el derecho a la libertad de pensamiento, control sobre nuestro cuerpo, soledad en nuestro hogar, control sobre la información personal, el derecho a no ser vigilado, protección a la reputación y protección de pesquisas e interrogatorios. Cabe reconocer que el derecho a la privacidad no es necesariamente apoyado de manera unitaria en la doctrina. Eipstein (1994) considera que la privacidad es la súplica por el derecho a tergiversar la imagen que tiene el mundo de nosotros.

Esta característica multifacética del derecho a la privacidad, aunado a la íntima relación que el mismo tiene con desarrollos tecnológicos, se traduce en un atraso de las normas tendientes a protegerlas. Durante la década de los años 60 y 70 se introduce el concepto moderno de privacidad fundamentado en un control de datos basado un aviso previo y consentimiento informado. Durante la misma época, las discusiones sobre la privacidad se van alejando de la esfera del derecho privado y comienzan las discusiones sobre los límites del poder estatal, particularmente en lo relativo a vigilancia e investigación de sus ciudadanos. Surgen nuevos conceptos, como el de la expectativa razonable de privacidad, introducido en el caso Katz v. U.S.(Katz;U.S., 2967, p. 361) [2], y que has servido como el fundamento jurídico de la privacidad en el derecho estadounidense.

La introducción de tecnologías computacionales 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 contrapone 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 reavivo las discusiones sobre el concepto o de privacidad, en donde las teorías clásicas desarrolladas para tecnologías análogas no se adaptan programas de ordenador, en una sociedad donde la información se ha convertido en una moneda más. Las discusiones ya no solo se centran en el control de los datos, sino que abarcan la posibilidad de un derecho de propiedad sobre los mismos, una clara contraposición sobre la idea original propuesta por Warren y Brandeis.

Ya para 1996, Mell (1996) 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 científico (Determan, 2018). Esta dinámica privacidad-innovación retoma mayor importancia en un mundo moderno basado en ciudades inteligentes.

2. Katz v. U.S., 389 U.S. 347, 361 (1967).

II. La Sociedad Inteligente

i. El surgimiento de las ciudades inteligentes

En la actualidad aún no es posible hablar de una sociedad inteligente. 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 que constituye una ciudad inteligente existen una serie de elementos comunes que las distinguen. Para Cugurullo (2018), 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, energía renovable, etc.

Kichin (2015) considera que existen 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.

Independientemente de la definición que se elija, una ciudad inteligente 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, etc. [Mehmood, Bhaduri, Katib, Chlamtac, 2018]. 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.

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.

La estructura de una sociedad inteligente ya sea a nivel general o de ciudades, hace necesaria una gran cantidad de información para que la misma pueda funcionar de manera óptima. Edwards (Edwards, 2016) 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, macro datos, 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.

a) El internet de las cosas (IoT)

El termino internet de las cosas (IoT por sus siglas en inglés[3]) se refiere a un sistema de dispositivos conectados a una red o unos a otros sin que sea la necesidad una interacción humano-maquina (CRS, 2019). Una característica esencial de los dispositivos IoT es que son personalizables, el usuario debe proveer información a fin de utilizar todas las funciones a máximo. Cabe destacar que dispositivos como computadoras, tablets y smartphones requieren, por diseño, estar conectados a una red para ser utilizados por lo que no suelen ser considerados como parte del IoT. En cambio, los dispositivos IoT hacen uso de la red para mejorar su rendimiento o proporcionar al usuario funciones extras, por ejemplo, un refrigerador que determine cuando falta un ingrediente, un termostato que ajuste la temperatura a cierta hora o bien un vehículo inteligente capaz de conducirse solo. Las proyecciones sobre la implementación de tecnologías IoT no son uniforme. La compañía de telecomunicaciones Ericsson estima que para el año 2022 unos 18 billones de dispositivos estarán conectados al internet de las cosas (Ericsson, s.f.). Por su parte, Cisco, considera que para 2030 el número de dispositivos alcanzara los 500 billones (CISCO, 2016).

El IoT se presenta casi como una panacea, con aplicaciones en sectores que van desde servicios de salud hasta seguridad nacional. Pero quizás su mayor impacto puede observarse en la vida diaria de ciudadanos ordinarios, con sensores que detectan el nivel de energía de una residencia, hasta dispositivos que pueden conectarse al teléfono del individuo para medir el nivel del alcohol en la sangre. Independientemente de la forma en que se presenten, la característica esencial de estos dispositivos es el uso de datos, por lo que surgen interrogantes sobre el nivel de protección a la privacidad de los usuarios.

Antes de continuar es necesario establecer los límites de nuestro argumento. Este escrito se limita a las tecnologías IoT desde la relación consumidor-comercio y, en algunos casos, ciudadano-gobierno. Las tecnologías IoT son una parte esencial de procesos transporte, almacenaje y otros procesos industriales como lo son líneas de ensamblaje. Este tipo de tecnologías no son el objeto de este artículo, por cuanto si bien las mismas pueden recolectar información sobre los empleados de una empresa determinada, esto se realiza dentro del marco de sus labores ordinarias dentro de la propiedad de la empresa en cuestión. Por ende, puede argumentarse que el empleado está sometido a las reglas internas del comercio y debe desenvolverse acordemente.

Esto no quiere decir que todas las interacciones con tecnologías IoT dentro de un marco laboral están exentas de escrutinio. Existen un sin número de negocios que proporcionan a sus empleados con tecnologías IoT para su uso personal, o bien que requieren que el empleado cargue el dispositivo en su persona a toda hora. En estos casos los límites de la relación empleado-empleador de desdibujan a un punto donde es posible tratarlas de la misma manera que una violación de privacidad entre dos individuos particulares.

Edwards (2016) describe el dilema IoT y privacidad de manera puntual. Cuando un usuario proporciona sus datos en línea en plataformas como Facebook, Google, Amazon, etc., lo hace siendo consciente, aunque este conocimiento es escaso en ocasiones, de que se cruza un lumbral hacia el dominio de la plataforma, y con la oportunidad de dar su consentimiento para la recolección de sus datos antes de utilizar el servicio. En las tecnologías IoT tal oportunidad se encuentra ausente por

3. El primer uso del término se le atribuye a Kevin Ashton en su presentación That 'Internet of Things' Thing en 1999.

diseño, ya que los dispositivos suelen ser pequeños, carecer de pantallas o de algún mecanismo que permita al usuario dar su consentimiento.

Las tecnologías IoT deben ser invisibles para ser eficaces, un dispositivo IoT que requiera el consentimiento del usuario cada vez que trate de recolectar información pierde su razón de ser, en parte porque no todos los usuarios cuentan con el nivel de educación tecnología necesaria para comprender lo que se pide de ellos. En algunas ocasiones el usuario puede no tener opción. Un ejemplo claro son los vehículos inteligentes. Para que el vehículo funcione de manera adecuada es necesario que el mismo intercambie información con otros vehículos en la vía, y en algunos casos, con dispositivos de control sobre la carretera.

Peppet (2014) comenta que aun los dispositivos IoT más inocuos pueden producir grandes cantidades de datos sobre los usuarios, y estos datos, una vez filtrados mediante tecnologías analíticas pueden ser usados para revelar la personalidad, hábitos y predilecciones de los usuarios. Datos sobre consumo eléctrico pueden revelar a qué hora se despierta o duerme un individuo, así como a qué hora sale de su residencia al trabajo. Una pulsera o reloj que mida la actividad física puede revelar no solo el estado de salud del usuario sino también sus rutas preferidas por medio del GPS. No es necesario forzar la imaginación para concebir usos a esta información. Solo en los servicios médicos las tecnologías IoT están siento utilizadas para medir el efecto de medicamentos en pacientes de Parkinson y esclerosis múltiple (Dimitrov, 2016). Sin embargo, la misma data puede ser utilizada en industrias como seguros y préstamos bancarios para determinar la viabilidad de un cliente, creando un perjuicio en contra de personas que decidan no adoptar este tipo de tecnologías.

En estos casos la pregunta de quién es dueño de los datos es de vital importancia. A diferencia de aplicaciones y programas de ordenador, la gran mayoría de los dispositivos IoT no incluyen una política de privacidad en sus manuales de uso y en muchos casos se limitan a dirigir al usuario a sitios de internet en donde se encuentra esta información. Más aún, cualquier cambio en estas políticas de privacidad se realiza sin conocimiento del usuario, quien no requiere una pantalla para utilizar el dispositivo IoT.

A nivel de la profesión legal, los contratos relativos a tecnologías IoT presentan una seria de desafíos que no suelen encontrarse en otras ramas. Noto de La Diega y Walden (2016) explican que los contractos sobre IoT son difíciles de entender por cuatro motivos. En primer lugar, el uso de términos tecnológicos y jurídicos convierten a los contratos de un contrato de IoT requiere un alto nivel de conocimiento en ambas ramas. Segundo, de la misma manera que las leyes, los contratos sobre IoT son escritos cuando las tecnologías se encuentran en desarrollo, por lo que en muchas ocasiones no pueden ser utilizados con nuevas tecnologías. En tercer lugar, está el hecho de que los contratos suelen redactarse con las normas de Estados Unidos en mente, y en muchas ocasiones no son adaptados a otras jurisdicciones. Finalmente, el mercado de IoT se caracteriza por sus múltiples capas, lo que se convierte en un obstáculo a la hora de determinar que contrato es aplicable a una situación particular.

b) Big Data

La información recolectada por dispositivos IoT no es, por misma, suficiente para el buen funcionamiento de una ciudad inteligente. Dicha información no es más que una materia prima y únicamente cuando se usa en conjunto con tecnologías y algoritmos de macro datos (*Big Data)* puede ser utilizada al máximo. En sí, el termino

macro datos se presta para confusión. Como lo expresan Boyd y Crawford (2011), la característica principal de los macro datos no es la cantidad de los datos, sino la relación que guarda con otros tipos de datos. Su valor radica en los patrones de conducta que pueden inferirse en base la información recolectada.

Dentro del engranaje de una ciudad inteligente, la información recolectada es procesada mediante el uso de macro datos, y su uso no se limita a toma de decisiones a nivel de instituciones gubernamentales, extendiéndose a servicios médicos, operaciones de transporte y agencias de publicidad son solo algunos ejemplos del tipo de negocios que utilizan macro datos para analizar las conductas de sus clientes y posibles socios. No obstante, el existen críticas sobre el uso de macro datos no solo desde la perspectiva de privacidad sino también sobre la protección de derechos civiles.

En teoría, estos datos deben ser anonimizados antes de ser utilizados dentro de las estructuras de las ciudades inteligentes. Esto puede llevar a que se consideres como fuentes confiables de toma de decisiones neutrales. Un reporte de 2016 de la Oficina del presidente de los Estados Unidos (EotP, 2016) describe dos maneras en los que los algoritmos encargados de procesar los datos pueden ser afectados. La primera es durante la introducción de los datos al sistema. Debido a que un sistema puede utilizar diversos datos al momento de tomar una decisión, los datos que sirven como base pueden cambiar el resultado. Esto puede darse cuando los datos no son adecuados, cuando los mismos están incompletos o son obsoletos, cuando la recolección de datos en si sufra de prejuicios o bien cuando los datos puedan usarse para justificar acciones contra un cierto grupo.

Si bien los macro datos pueden utilizarse para mejorar la productividad de un negocio en particular tomando en cuenta las características de sus clientes a fin de ofrecerles un producto que se adapte a sus necesidades, el hecho de que la toma de decisiones se realiza mediante procesos algorítmicos ha producido discusiones en la doctrina sobre la posibilidad de prejuicios ocultos en los estos procesos. Estos sistemas utilizan una seria de relaciones entre datos denominadas "modelos" para llegar a un resultado. En términos sencillos, el modelo es una operación que le permite al sistema utilizar los datos proporcionados para presentar una solución a una consulta.

Los datos que el sistema uso como guía se denominan datos de entrenamiento (*training data)*. Barocas y Selbst (2016) explican diversas formas en las que un modelo puede verse comprometido. En primer lugar, es posible que el modelo se vea afectado de manera originaria, es decir, que diseño del modelo contenga una falla que no haya sido detectada. Puede darse el caso de que el algoritmo este mal diseñado, que sean utilizado para reducir las opciones del usuario, que asuman elementos de causalidad sin que existan pruebas de tal relación. Debido a que muchos de estos algoritmos están protegidos mediante leyes especiales o por sistemas de propiedad intelectual, los usuarios se enfrentan a una serie de obstáculos en el caso de que soliciten una apelación a una decisión basada en los mismos. También es posible que algunos casos la integración del algoritmo con otros sistemas impida que el mismo pueda ser modificado sin afectar a otros individuos o transacciones.

La segunda manera en la que un algoritmo puede verse afectado es por acciones de los usuarios. En específico, es posible que los datos de entrenamientos sean clasificados de manera incorrecta por la persona encargada de introducirlos al sistema.

Esto incluye meros errores de contenido, como puede ser ortografía, así como situaciones que requieren de la interpretación humana. Esta situación se da en sistemas que realizan operaciones de impuestos. La determinación de si un pago se constituye como gasto de negocio debe hacerla el individuo que utiliza el sistema, en base a sus conocimientos de las normas fiscales. El modelo en si no puede tomar esa decisión, simplemente puede calcular la carga impositiva en base a los datos que le han suministrado. Una situación similar se da con la veracidad de la información recolectada. El sistema solo puede proporcionar una respuesta en base a las variables que se le presenten, si una de esas variables no resulta confiable por errores humanos, la respuesta que resulte será errónea.

Un ejemplo reciente que trajo esta discusión a la palestra es la implementación en el estado de California, Estados Unidos, de sistemas algorítmicos para determinar la viabilidad de otorgar libertad bajo fianza a individuos privados de libertad. El nuevo sistema remplaza la fianza monetaria impuesta por jueces por un sistema algorítmico que toma en cuenta varios factores al momento de decidir si un individuo puede ser beneficiado con una medida de libertad condicional (The Guardian, 2018).A pesar de que este nuevo proceso de fianza fue introducido como una solución a los problemas de detención preventiva, y que sus promotores proclaman que el algoritmo ayudará a reducir prejuicios raciales contra individuos de color, el mismo ha sido objeto de diversas críticas. El diseño del algoritmo no está establecido en la ley, los datos utilizados por el sistema son recopilados de los informes policiales, que a su vez pueden estar viciados por prejuicios raciales que no son evidentes a simple vista.[4]

Balkin (Balkin, 2017) utiliza el termino sociedad algorítmica (*Algorithmic Society*) para referirse a una sociedad en donde las decisiones económicas y sociales se toman en base a sistemas algorítmicos. Balkin continúa explicando que uno de los mayores desafíos de una sociedad algorítmica es lo que él denomina la falacia del homúnculo (*homunculus fallacy*), que no es más la imagen equivocada de la maquina es contralada por un actor semihumano, que obliga al sistema a dar buenos o malos resultados. En otras palabras, los humanos solemos humanizar los modelos algorítmicos para explicar por qué el sistema llega a una conclusión en particular.

Sin embargo, y como bien lo apunta Balkin, los sistemas algorítmicos, ya sean que hagan uso de macro datos o de tecnologías de la nube, solo son capaces de realizar las operaciones para las que fueron programados. El modelo no es capaz de dar una respuesta para la cual no ha sido programado. Por ende, uno de los mayores temores de sistemas que utilicen modelos algorítmicos para la toma de decisiones, ya sea a nivel comercial o, como el caso de California, a nivel de justicia penal, es que el sistema revele prejuicios inherentes no solo en los datos sino en nuestra sociedad.

Desde ámbito de la privacidad, los sistemas algorítmicos de macro datos presentan una serie desafíos en relación con decisiones jurisdiccionales. Un ejemplo claro de esta situación se da con el derecho al olvido (*right to be forgotten)* que tuvo su origen en la Unión Europea. Villaronga *et al* (Fosch Villarongaa, Kiesebergb, & Li, 2018) exponen como una decisión judicial de eliminar una información determinada, puede no resultar práctica desde un punto de vista técnico. Las bases de datos actuales utilizan reglas ACID (*Atomicity, Consistency, Isolation and Durability*) que aseguran su estabilidad y confiabilidad. Una característica esencial de estos sistemas es su integración,

4. Cabe señalar que muchas de las críticas al nuevo sistema se centran en elementos legales y no técnicos. Por ejemplo, bajo la nueva ley un individuo puede ser caracterizado como de bajo, medio o alto riesgo. La norma solo permite la fianza para individuos de bajo o medio riesgo. Sin embargo, algunos delitos no son susceptibles de fianza, lo que significa que, en teoría, un individuo puede permanecer detenido preventivamente si la fiscalía lo acusa de uno de estos delitos, sin que el juez pueda tomar en consideración las circunstancias del caso en particular (Washington Post, 2018).

sin entrar a consideraciones técnicas, los mismos están diseñados para funcionar como un todo, por lo que eliminar una variable del sistema, como lo es los datos de un individuo, puede afectar otros elementos de maneras no previsibles.

Por último, queda la interrogante de si es posible anonimizar un dato de manera absoluta en mundo con la capacidad computacional de las sociedades modernas. El problema no radica en la capacidad de desasociar un dato determinado con su particular, sino en la cantidad de datos recolectados permitan la identificación del titular mediante su análisis combinado. Solove (2013) describe esta situación como el problema de la agregación (*the problem of aggregation*). En el ámbito tecnológico se utiliza el término "*sensor fusion*" para definir el fenómeno donde datos de dos dispositivos que no se encuentran conectados pueden producir una mayor cantidad de información en conjunto que la suma de sus partes (Peppet, 2014).

Esta situación cobra aún más importancia cuando se considera el rol de entes particulares en las ciudades inteligentes. Como lo expone Edwards (Edwards, 2016), el hardware utilizado para el procesamiento de macro datos suele ser propiedad de compañías privadas, autorizadas por el Estado. Sadowski y Bendor (Sadowski & Bendor, 2019) revelan como dos compañías: IBM y CISCO controlan el negocio de componentes utilizados para las ciudades inteligentes, y como resultado pueden influir en el desarrollo de este tipo de centros urbanos, al punto de que la ciudad de Sogndo en Corea del Sur, puede considerarse como una ciudad construida por CISCO debido al gran número de contratos que ha celebrado para la instalación y administración de sistemas inteligentes.

En la actualidad muchos de estos servicios inteligentes son optativos, proporcionando una alternativa no inteligente. Por ejemplo, ciudades con servicios de transporte publico pueden ser utilizados tanto con dinero en efectivo como con tarjeta. La tarjeta le proporciona al usuario facilidades del uso del servicio público. A cambio, la empresa, o la entidad estatal obtiene la información sobre el uso del sistema. En la medida que la información se recolecte de manera anónima el sistema no infringe el derecho del usuario. Esta información permite optimizar los servicios de manera que la comunidad en general se beneficia sin que exista un alto riesgo para el ciudadano o usuario.

La historia reciente, en particular la crisis económica de 2008-2009, nos demuestra como un alto nivel de dependencia a un tipo de servicios puede afectar a una sociedad en cuando el sistema falla. En el caso de la crisis económica, el efecto se sintió en la disponibilidad de crédito y otros instrumentos financieros. Si la integración tecnológica de las ciudades inteligentes se limita a pocas compañías, se corre el riesgo de que el correcto desempeño de estas sea necesario para el adecuado funcionamiento de la sociedad.

No obstante, puede argumentarse de que en la actualidad existen modelos similares, en particular en lo que se refiere a la distribución de energía eléctrica o servicios de telecomunicaciones. La diferencia radica en el tipo de control que estas compañías pueden ejercer sobre los usuarios. Las compañías que controlen las herramientas de procesamiento de macro datos no solo proporcionan un servicio público, sino que tendrían acceso a una gran cantidad de información personal de cada uno de sus usuarios, lo que supondría un mayor riesgo para la seguridad y privacidad individual de cada uno de ellos.

c) La computación en la nube

Existen dos definiciones sobre que constituye servicios computacionales en la nube. La primera, es la definición del Instituto Nacional de Estándares y Tecnología (NIST por sus siglas en inglés) de los Estados Unidos. El NIST define servicios computacionales en la nube como un modelo que permite, a petición del usuario, el acceso conveniente de una red de recursos computacionales configurables (v.gr. redes, servidores, almacenamiento, aplicaciones, servicios) los cuales pueden ser provistos y liberados rápidamente con un mínimo esfuerzo administrativo o interacción del proveedor del servicio (NIST, 2018). A nivel internacional, la Organización Internacional de Normalización (ISO por sus siglas en inglés) pero medio del Comité Conjunto Técnico, en la norma ISO/IEC 17788:2014, define los servicios de computación en la nube como paradigma para permitir el acceso a la red a un grupo de recursos ajustables y elásticos que pueden ser físicos o virtuales que pueden ser compartidos (ISO, 2014).

Independientemente de la definición que se elija, los servicios de computación en la nube comparten una seria de caracterizan esenciales (Microsoft, 2017). En primer lugar, estos servicios son de acceso amplio, permitiendo que varios usuarios accedan, y en muchos casos, modifiquen la información de manera simultánea. Son servicios cuantificables, por cuanto, como regla general, los usuarios solo pagan por la cantidad de servicio utilizada. Igualmente, el acceso a los recursos se realiza en base a grupos, por ejemplo, dos compañías pueden tener acceso a un servidor, pero el uso que pueden darle se limita a los permisos de su grupo. Otra característica esencial del servicio es la independencia, puesto que el usuario no requiere interactuar con el administrador del servicio en la mayoría de los casos. Aunado a esto, la computación en la nube se ajusta a las necesidades del usuario pudiendo expandirse o reducirse a la medida que se requiera. Finalmente, los servicios de computación en la nube permiten el uso conjunto de los recursos para satisfacer las necesidades del cliente.

De los tres elementos identificados por Edwards, los servicios de tecnología de nube pueden enmarcarse en las teorías tradicionales de consentimiento para el uso de datos personales. Estos servicios son similares a otros programas de ordenador en tanto los mismo requieren que el usuario creé una cuenta y acepté los términos de uso para poder acceder al servicio. A nivel de uso personal, los servicios de almacenaje en la nube no difieren de otros servicios similares de transferencia o almacenamiento de datos, y en la mayoría de los casos el usuario conserva la propiedad intelectual sobre sus datos. Sin embargo, una característica común de este tipo de servicios, y que se extiende a redes sociales como Facebook, es que el usuario les otorga a las compañías una licencia de uso de los datos.[5]

No obstante, su función en una ciudad inteligente no se limita al almacenamiento de datos. La principal función de estos servicios es facilitar la recolección de información mediante tecnologías IoT y coadyuvar a su procesamiento por medio de algoritmos de macro datos. Sin la ayuda de computación en la nube una compañía debe invertir en la infraestructura necesaria para poder procesar los datos recolectados.

5. Por ejemplo, las Condiciones del servicio de Google Drive en su artículo 2 establecen lo siguiente:
Su contenido. Google Drive le permite subir, ingresar, almacenar, enviar y recibir contenido. Usted conservará los derechos de propiedad intelectual que posea sobre él. En resumen, lo que le pertenezca continuará siendo suyo.
Cuando suba, ingrese, almacene, envíe o reciba contenido en Google Drive o por medio de él, otorgará a Google **una licencia internacional para utilizar, alojar, almacenar, reproducir, modificar, crear obras derivadas (como las traducciones, adaptaciones o modificaciones que hagamos para que su contenido funcione mejor con nuestros servicios), comunicar, publicar, ejecutar o mostrar públicamente, y distribuir** dicho contenido. Los derechos que usted otorga en esta licencia son para el objetivo limitado de operar, promocionar y mejorar nuestros servicios, y para desarrollar otros nuevos. Esta licencia seguirá vigente aun cuando deje de utilizar nuestros servicios, a menos que borre su contenido. Asegúrese de tener los derechos necesarios para otorgarnos esta licencia respecto de cualquier contenido que envíe a Google Drive. (el resaltado es nuestro).

Desde el punto de vista del usuario, el uso de sistemas en la nube implica que los datos pueden ser procesados en una escala nunca antes posible, multiplicando tanto los posibles beneficios como los riesgos implícitos. Por ejemplo, el usuario no tiene control del lugar físico donde se almacenan sus datos, limitando la posibilidad de obtener remedio legal en caso de infracciones a sus derechos. Como consecuencia, existen discusiones sobre la introducción del concepto de residencia de data (*data residence*) o localización de data (*data localization*), el cual implica que los datos personales de un individuo deben ser almacenados en un servidor bajo la jurisdicción de su Estado nacional.

En la actualidad, la discusión sobre el libre flujo de información se divide en dos frentes: uno liderado por Estados Unidos, que propone una libertad absoluta de intercambio de información, y el otro, representado por China, que aboga por un control absoluto del Estado sobre la información de sus nacionales (Reinsch, 2018). Sin embargo, muchos países adoptan posturas eclécticas, como lo es el caso de Corea del Sur, que limita la transferencia de ciertos datos como lo son modelos geográficos, que por motivos de seguridad nacional deben almacenarse dentro de territorio coreano. La ley de datos griega de 2001 requiere que los datos recolectados en Grecia sean almacenados dentro del territorio nacional, Dinamarca tiene reglas similares para la información financiera de sus nacionales.

Recientemente en Alemania, el uso de los programas de ordenador bajo la marca Office de Microsoft han sido prohibidos en las escuelas primarias porque recolectaban información personal de los estudiantes (Salter, 2019). Normalmente, el usuario de da su consentimiento al momento de instalar o utilizar los programas de Office, permitiendo la recolección de datos personales. Sin embargo, en el caso alemán, los usuarios son menores de edad cursando estudios elementales, por lo que legalmente, no tienen la capacidad jurídica para dar su consentimiento.

III. La privacidad en una Ciudad Inteligente

i. El dilema del consentimiento

En una sociedad cada más dependiente de los datos para poder funcionar el derecho de privacidad se enfrenta a un dilema en cuanto consentimiento en la difusión de datos. Daniel Solove (2013) propuso el termino 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, ya sea bajo Warren-Brandeis 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 (*privacy self-management*), las cuales se remontan a las *Fair Information Practices Principles* 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 (Solove, 2013).

Solove identifica varios desafíos que enfrenta la teoría de la autogestión de privacidad en una sociedad basada en los macro datos. En primer lugar, existe el problema de *toma de decisiones distorsionada (skewed decisión-making)*. Este problema se manifiesta en el hecho de que la mayoría de los individuos no leen las políticas de privacidad relativas al uso de sus datos, y aun en el caso de que las leyeran, no poseen los conocimientos necesarios para poder comprenderlas. Proponentes del sistema de autogestión abogan por el uso de lenguaje simple en las políticas de privacidad, y varias legislaciones, como la GDPR europea y la Privacy Act americana siguen este principio. Sin embargo, el uso de lenguaje simple se erige como una paradoja que impide la aplicación del principio. Por una parte, una simplificación exagerada de los términos de privacidad corre el riesgo de no ser lo suficientemente específica para informar al titular del uso que se les dará a sus datos, en efecto negando el principal objetivo de dichas políticas.

Existen también los problemas de escala (*problema of scale)* y el problema de la acumulación (*problema of aggregation)*. Estos problemas tienen su origen en el hecho de que la cantidad de entidades y organizaciones que hacen uso de los datos personales aumentan constantemente. Un individuo puede, en teoría, llevar un control del número de veces que ha proporcionado información personal, en un sistema basado en métodos tradicionales no digitales. Sin embargo, en la sociedad moderna, el número de entidades es tal que no es posible que un individuo conserve un conteo sobre la cantidad de datos que ha proporcionado, así como el contenido de cada uno de ellos. No obstante, los datos recolectados son por lo general datos anónimos o anonimizados, y la privacidad siempre ha tenido como objeto la protección de información personal identificable. Aunado a estos problemas Solove también identifica el problema de la determinación del daño (*problema of assesing harm)* o la dificultad del titular en juzgar correctamente el daño que pueda sufrir producto proporcionado sus datos.

Una vez el titular ha dado su consentimiento, las protecciones otorgadas por el derecho a la privacidad dejan de surtir efecto. Sin embargo, este esquema resulta adecuado para un sistema recolección o publicación de datos basado en medios físicos o programas de ordenador, no lo es para tecnologías IoT, que requieren ser de fácil uso al punto que resulten casi invisibles para el usuario en su vida diaria. Una vez la información se transfiere a un medio digital, el control del individuo sobre la misma se pierde completamente.

Varias soluciones se han presentado para enfrentar este dilema. Algunos autores como Luger y Rodden (2013) argumentan que el consentimiento debe ser interpretado como un proceso continuo, abandonando las teorías actuales bajo las cuales el consentimiento solo se da al inicio de la recolección de datos. Otras soluciones hacen uso de la tecnología para otorgarle al usuario un mayor control sobre su privacidad. Esta postura aboga por un centro de control o *centro de operaciones* que le permita al usuario establecer unas reglas de uso de datos por defecto y, cuando un nuevo dispositivo se conecte a la red del usuario, el mismo será programado con las preferencias de privacidad preestablecidas. Este concepto se conoce como consentimiento semiautónomo (*semi-autonomous consent*) o preconsentimiento (Gomer, Schraefel, & Gerding, 2014).

En Europa, algunos autores propugnan por 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 informado

(Edwards, 2016). 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 tecnologías. Un ejemplo claro de esto fue el "*Google Glass*", un dispositivo que se proponía ser un centro de operaciones digital para los usuarios y que sin embargo fue abandonado producto del poco interés que produjo en la sociedad en general, a pesar de su popularidad en círculos tecnológicos (The Week, 2015). Recientemente, la tecnología ha reaparecido en una versión para negocios (Tiwary, 2019).

ii. La privacidad y los espacios públicos

Otro desafío importante en una ciudad inteligente es la relación entre privacidad y espacios públicos. Tradicionalmente, el derecho a la privacidad y las reglas referentes al consentimiento no se extienden a espacios públicos, donde el individuo no cuenta con ningún tipo de expectativa de privacidad. El desarrollo tecnológico de la era digital ha traído como resultado la expansión del concepto de espacio público que no era posible prever hace 50 años. Algunos países, como Inglaterra, se caracterizan por la poca protección que un individuo tiene sobre su privacidad una vez salga de su residencia. En el caso inglés, la gran cantidad de cámaras de vigilancia hacen imposible que una persona pueda tener una expectativa razonable de seguridad, bajo el argumento de la seguridad.

Este argumento no es nuevo, y se ve reflejado en países que son víctimas de algún tipo de ataque, ya sea interno o externo, o que ejercen un gran nivel de control sobre la vida de sus ciudadanos y visitantes. Sin embargo, en los últimos años, el nivel de escrutinio por parte de algunos estados conlleva que las discusiones sobre la privacidad no se limiten al ámbito del derecho privado, extendiéndose a la rama de los derechos humanos.

El concepto de espacio público también se verá afectado en una sociedad basada en tecnología inteligente. En particular la introducción de drones has puesto en entredicho 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 urbanas, 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 (Nippon, 2019).

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 tomar dar un solo paso" (ABC news, 2018).

En baso a los datos recolectados, cada individuo recibe un récord de crédito en base a sus acciones (Kobie, 2019). Bajo el plan actual, cuando el "puntaje" de un individuo baja de cierto "nivel" el mismo se convierte en blanco de una serie de sanciones como lo son la imposibilidad de abordar aviones o trenes, adquirir derechos sobre propiedad privada, ser sujeto de crédito hipotecario, la expulsión del individuo, o sus hijos, de escuelas de prestigio, la imposibilidad de ocupar cargos de administración en instituciones del estado o compañías con participación estatal, ser nombrado un mal ciudadano, entre otras (Ma, 2018).

Al momento de redactar este artículo el sistema se encuentra en fase de prueba, sin que exista una versión unitaria. Cada región de China cuenta con un sistema diferente, pero conservando las mismas características generales. Existen también modelos privados, utilizados principalmente por empresas para determinar la credibilidad de sus clientes. Cuando el plan sea implementado en su totalidad se espera que todos estos sistemas se unan bajo un mismo sistema general nacional, vinculado al número de identidad personal de cada individuo. La provincia de Heibei, en el norte de China, ha creado una aplicación que hace uso de los datos del sistema de crédito social para informar a sus usuarios si se encuentran cerca de un individuo que no haya pagado una deuda a pesar de existir una decisión judicial en firme (Ma, 2019). En otras provincias, llamar al teléfono de un individuo dentro de la lista de morosos significa escuchar un mensaje animando a la persona que llama a que convenza al moroso para que pague su deuda (Campbell, 2019).

iii. La privacidad como un concepto social

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. 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, el europeo y estadounidense, no están fundamentados en los mismos principios.

Cohen (2013) considera que la privacidad se convierte en una herramienta para que el individuo pueda auto superarse, sin la influencia critica de la sociedad que le rodea. La privacidad es un elemento importante de las democracias liberales, por cuanto una sociedad basada en una vigilancia constante del individuo por cuanto permite que el mismo desarrolle una visión crítica de la sociedad.

El concepto de privacidad también refleja particularidades políticas, históricas y sociales. El ejemplo más claro de puede observarse en los dos grandes sistemas de privacidad occidentales: el europeo y el estadounidense. 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. Whitman (2004), explica como el concepto de privacidad europeo y estadunidense tienen distintos origines. La modelo europea 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. Sin embargo, y a pesar de la imagen orwelliana que presenta el sistema de crédito social chino, Kostka (Kostka, 2019), 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 de sobre el apoyo al sistema puede 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.

IV. Conclusiones

La privacidad va de la mano con los desarrollos tecnológicos de cada época. Las limitaciones físicas que sirvieron de fundamento a las reglas de la teoría clásica no existen en la era digital, donde los usuarios proporcionan información personal a

diario sin que sean conscientes de exactamente 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 macro 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 globalizado, en particular uno basado en un la conección de ciudades inteligentes, 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 informatico 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 método optimo para proteger los derechos de los 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.

Referencias

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

Balkin, J. M. (2017). The three laws of robotics in the age of Big Data. *Ohio State Law Journal, 78*(5), 1217-1241.

Barocas, S., & Selbst, A. D. (2016). Big Data´s disparate impact. *California Law Review, 104*, 671-732.

Boyd, D., & Crawford, K. (2011). Six provocations for Big Data. *A Decade in Internet Time: Symposium on the Dynamics of the Internet and Society.* Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1926431

Campbell, C. (2019). *How China is using "Social Credit Scores" to reward and punish Its citizens*. Recuperado el 11 de septiembre de 2019, de time.com: https://time.com/collection/davos-2019/5502592/china-social-credit-score/

CISCO. (2016). *Internet of Things.* Recuperado el 5 de septiembre de 2019, de cisco.com: https://www.cisco.com/c/dam/en/us/products/collateral/se/internet-of-things/at-a-glance-c45-731471.pdf

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

CRS. (2019). *Internet of Things: an Introduction.* Congreso de los Estados Unidos, Congressional Research Service. Recuperado el 11 de septiembre de 2019, de https://crsreports.congress.gov/product/pdf/IF/IF11239

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;.

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

Dimitrov, D. V. (2016). Medical Internet of Things and Big Data in healthcare. *Healthcare Informatics Research, 22*(3), 156-163.

EC. (s.f.). *Smart cities: Cities using technological solutions to improve the management and efficiency of the urban environment.* EC. Recuperado el 26 de agosto de 2019, de https://ec.europa.eu/info/eu-regional-and-urban-development/topics/cities-and-urban-development/city-initiatives/smart-cities_en#related-policies

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

Eipstein, R. (1994). The legal regulation of genetic discrimination: old responsed to new techonology. *Boston Universtity Law Review, 74*(1), 1-23.

EotP. (2016). *Big Data: a report on algorithmic systems, opportunity, and civil rights.* Executive Office of the President, Washington. Retrieved from https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/2016_0504_data_discrimination.pdf

Ericsson. (n.d.). *The connected future*. Retrieved septiembre 5, 2019, from https://www.ericsson.com/en/mobility-report/internet-of-things-forecast

Fosch Villarongaa, E., Kiesebergb, P., & Li, T. (2018). Humans forget, machines remember: artificial intelligence and the right to be forgotten. *Computer Law & Security Review, 34*, 304-313.

FTC. (2015). *Internet of Things privacy & security concerns in a connected world.* Federal Trade Commission. Retrieved 8 26, 2019, from https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf

Gomer, R., Schraefel, M., & Gerding, E. (2014). Consenting agents: semi-autonomous interactions for ubiquitous consent. *UbiComp'14: How Do You Solve a Problem like Consent?*, (pp. 653-658). Seattle.

ISO. (octubre de 2014). Recuperado el 11 de septiembre de 2019, de ISO: https://www.iso.org/obp/ui/#iso:std:iso-iec:17788:ed-1:v1:en

Kitchin, R. (2015). *The promise and perils of Smart Cities*. Recuperado el 15 de septiembre de 2019, de SCL: https://www.scl.org/articles/3385-the-promise-and-perils-of-smart-cities

Kobie, N. (2019). *The complicated truth about China's social credit system*. Recuperado el 11 de septiembre de 2019, de WIRED: https://www.wired.co.uk/article/china-social-credit-system-explained

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

Luger, E., & Rodden, T. (2013). An informed view on consent for UbiComp. *Proceedings UbiComp '13 , Proceedings of the 2013 ACM international joint conference on Pervasive and ubiquitous computing*, (pp. 529-538). Nueva York.

Ma, A. (2018). *China has started ranking citizens with a creepy 'social credit' system — here's what you can do wrong, and the embarrassing, demeaning ways they can punish you*. Recuperado el 15 de septiembre de 2019, de Business Insider: https://www.businessinsider.com/china-social-credit-system-punishments-and-rewards-explained-2018-4

Ma, A. (2019). *China reportedly made an app to show people if they're standing near someone in debt — a new part of its intrusive 'social credit' policy*. Retrieved septiembre 15, 2019, from Business Insider: https://www.businessinsider.com/china-app-shows-map-of-people-in-debt-for-social-credit-system-report-2019-1

Mehmood, R., Bhaduri, B., Katib, I., & Chlamtac, I. (Eds.). (2018). *Smart Societies, Infrastructure, Technologies and Applications: First International Conference, SCITA 2017, Jeddah, Saudi Arabia, November 27–29, 2017, Proceedings*. Springer.

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.

Microsoft. (2017). *An introduction to Cloud Computing for legal and compliance professionals.* Retrieved from Microsoft: https://download.microsoft.com/download/0/D/6/0D68AE95-6414-4074-B4B8-34039831E2BF/Introduction-to-Cloud-Computing-for-Legal-and-Compliance-Professionals.pdf

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

Nippon. (2019). *Japan enacts bill to ban drone flights over olympic venues*. Recuperado el 11 de septiembre de 2019, de Nippon.com: https://www.nippon.com/en/news/yjj2019051700536/japan-enacts-bill-to-ban-drone-flights-over-olympic-venues.html

NIST. (2018). *Cloud Computing*. Retrieved septiembre 5, 2019, from National Institute of Standards and Technology: https://csrc.nist.gov/projects/cloud-computing

Noto La Diega, G., & Walden, i. (2016). Contracting for the 'Internet of. *Queen Mary University of London, School of Law Legal Studies Research Paper No. 219/2016*.

Öman, S. (2004). Implementing data protection in law. *Scandinavian Studies in Law*(47), 389-403.

Peppet, S. R. (2014). Regulating the internet of things: first steps towards managing discrimination, privacy, security & consent. *Texas Law Review*, 85-176.

Reinsch, W. A. (2018, Marzo 9). *A Data Localization Free-for-All?* Retrieved from Center for Strategic & International Studies: https://www.csis.org/blogs/future-digital-trade-policy-and-role-us-and-uk/data-localization-free-all

Sadowski, J., & Bendor, R. (2019). Selling Smartness:Corporate Narratives and the Smart City as a Sociotechnical Imaginary. *Science, Technology, & Human Values*, 4(3), 540-563.

Salter, J. (2019). *Office 365 declared illegal in German schools due to privacy risks*. Recuperado el 15 de septiembre de 2019, de Arstechnica: https://arstechnica.com/information-technology/2019/07/germany-threatens-to-break-up-with-microsoft-office-again/

Science and Technology Policy. Council for Science, Technology and Innovation. (n.d.). *Cabinet Office*. Retrieved from Society 5.0: https://www8.cao.go.jp/cstp/english/society5_0/index.html

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

Solove, D. J. (2013). Privacy Self-Management and the Consent Dilemma. *Harvard Law Review*(156), 1880-1903.

The Guardian. (2018). *Imprisoned by algorithms: the dark side of California ending cash bail*. Recuperado el 15 de septiembre de 2019, de The Guardian: https://www.theguardian.com/us-news/2018/sep/07/imprisoned-by-algorithms-the-dark-side-of-california-ending-cash-bail

The Week. (2015). *Google Glass 'dead' as search giant shelves production*. Recuperado el 15 de septiembre de 2019, de theweek.co.uk: https://www.google.com/search?q=google+glass+shelved&oq=google+glass+shelved&aqs=chrome..69i57j69i64l2.3355j0j4&sourceid=chrome&ie=UTF-8

Tiwary, T. (2019). *Google Glass, long shelved for consumers, upgrades enterprise version*. Retrieved septiembre 15, 2019, from techcircle.com: https://www.techcircle.in/2019/05/21/google-glass-long-shelved-for-consumers-upgrades-enterprise-version

U.S. Department of Health, Education & Wellfare. (1973). *Record computers and the rights of citizens.* U.S. Department of Health, Education & Wellfare. Recuperado el 11 de septiembre de 2019, de https://www.justice.gov/opcl/docs/rec-com-rights.pdf

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

Washington Post. (2018). *California abolished money bail. Here's why bail opponents aren't happy.* Retrieved septiembre 15, 2019, from Washington Post: https://www.washingtonpost.com/news/monkey-cage/wp/2018/08/31/california-abolished-money-bail-heres-why-bail-opponents-arent-happy/

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