Anuario de Derecho N° 49-2020 – Año XL ISSN 0553-0814
Edición anual diciembre 2019-noviembre 2020
De la página 180 a la 190

I. AUTORES INTERNACIONALES INVITADOS

Del derecho de privacidad al derecho de protección de datos

RUBÉN E. RODRÍGUEZ SAMUDIO
Universidad de Hokkaido, Japón
Doctor en Derecho
E-mail: ruben18@juris.hokudai.ac.jp

RESUMEN

A pesar de su corta historia como parte del derecho privado, la privacidad es uno de los pilares en la sociedad moderna. Todo individuo tiene el derecho a desarrollar un pensamiento propio, aislado de críticas excesivas. Bajo esta perspectiva, el rol de la privacidad es otorgarle al individuo ese espacio para la reflexión. Sin embargo, el desarrollo tecnológico ha ejercido una gran influencia en el concepto de privacidad a lo largo de los años. En efecto, con cada nuevo avance en las tecnologías de la información, la percepción social de lo que puede considerarse privado evoluciona. En la actualidad nos encontramos frente ante las puertas de una nueva era. Una era caracterizada por una dependencia informática jamás vista, y que nos obliga a replantearnos la importancia de la privacidad en la sociedad del futuro.

Palabras Clave: Privacidad, Historia, Tecnología, Ciudades Inteligentes, Protección de Datos

ABSTRACT

Regardless of its short history as a private right, privacy is one of the pillars of modern society. Every individual has the right to develop their own thinking, without being the target of excessive criticism. Thus, the role of privacy is to grant individuals a place for reflection. Nevertheless, throughout the years, technological developments have always exerted great influence on the concept of privacy. Indeed, with each new advance of information technologies, the social perception of what can be considered private evolves. Presently, we are in the dawn of a new era. One characterized by an informational dependency of which the world has never seen, and that requires us to rethink the importance of privacy in future societies.

Keywords: Privacy, History, Technology, Smart Cities, Data Protection

Introducción

Este artículo describe la evolución de las doctrinas relativas a la protección de datos personales, iniciando por el derecho a la privacidad y concluyendo con las últimas tendencias en el derecho comparado dentro del marco de la era digital. En nuestro país, la Ley 81de 26 de marzo de 2019 de Protección de Datos Personales regula la materia. Sin embargo, muchas de las deficiencias del proyecto de ley, y de las cuales hicimos referencia en su momento se encuentran en el texto final. La privacidad como derecho no es uno de los puntos fuertes de la doctrina jurídica latinoamericana, una realidad a la que Panamá no escapa.

Aunado a esto, los avances tecnológicos de la última década han traído como resultado que las teorías tradicionales de la privacidad no sean aplicables en una sociedad informática. Actualmente, las sociedades modernas se encuentras experimentando un cambio trascendental. El desarrollo de tecnologías de recolección de información como el Internet de las Cosas (IoT), un aumento en la capacidad de procesamiento mediante el uso de tecnologías de Macro Datos (*Big Data*), y un incremento exponencial en la capacidad de almacenamiento y poder de computación

producto de la implementación de tecnologías de computación en la nube (*Cloud Computing)* han cambiado las reglas del juego.

Aunado a esto, los avances tecnológicos de la última década han traído como resultado que las teorías tradicionales de la privacidad no sean aplicables en una sociedad informática. Actualmente, las sociedades modernas se encuentras experimentando un cambio trascendental. El desarrollo de tecnologías de recolección de información como el Internet de las Cosas (IoT), un aumento en la capacidad de procesamiento mediante el uso de tecnologías de Macro Datos (*Big Data*), y un incremento exponencial en la capacidad de almacenamiento y poder de computación producto de la implementación de tecnologías de computación en la nube (*Cloud Computing)* han cambiado las reglas del juego.

Aún antes de la introducción de estas tecnologías, el concepto de privacidad como derecho no contaba con una estructura uniforme. Solove (2008) considera que la privacidad es un concepto desorganizado, por cuanto el mismo abarca, entre otras cosas, la libertad de pensamiento, el control sobre nuestro cuerpo, la soledad en nuestro hogar, control sobre la información personal, el derecho a no ser vigilado, la protección de nuestra reputación, y el derecho a no ser objeto de pesquisas o interrogatorios. Cohen (2013), explica que la privacidad es el espacio necesario para el desarrollo propio del individuo. En un mundo caracterizado por una cambiante y ubicua percepción social subjetiva, la privacidad le otorga al individuo un espacio donde le es posible desarrollar una perspectiva crítica del mundo.

Sin embargo, esta función de auto desarrollo que Cohen le otorga a la privacidad se ve afectada directamente por el nivel tecnológico de la sociedad de la que se hable. Esto es por cuanto, si bien la historia privacidad como concepto jurídico puede trazarse a las cortes de la Inglaterra medieval, no es sino hasta finales del siglo XIX cuando se puede hablar de la aparición de un derecho a la privacidad, y su desarrollo se ve afectado directamente por las tecnologías dominantes de la época.

En base a esto, el presente artículo se divide en 4 secciones: la primera se dedica a la introducción del concepto de privacidad iniciando partir del siglo XIX y culminando con la introducción de derechos análogos como el derecho a la publicidad durante la época de los años 1950. La segunda sección abarca el desarrollo del concepto moderno de privacidad, el cual tuvo su génesis producto de la recolección de datos personales por parte de actores estatales y se extiende hasta la época de los años 1980 con la introducción las tecnologías computacionales de uso particular. La tercera sección describe el surgimiento del concepto del control de datos personales y su importancia producto del desarrollo del internet durante la época de los años 1990. Finalmente, la cuarta sección plantea como la aparición de nuevas tecnologías de la información, afectan actualmente nuestra concepción del derecho de control de datos.

El origen de la privacidad como un derecho particular.

El desarrollo del derecho a la privacidad, y posteriormente al derecho de protección de datos, se encuentra íntimamente ligado a la jurisprudencia y doctrina estadounidense. Esto se debe a que la mayoría de las tecnologías que han servido como fundamento a las discusiones producto del desarrollo tecnológico han surgido de aquel país. Samuel D. Warren y Louis D. Brandeis (1890) fueron los primeros en analizar la naturaleza jurídica del derecho, la cual definen como el "derecho a ser dejado solo" (*the right to be left alone)*. Cabe señalar que Warren y Brandeis no crean el concepto de privacidad como una bien jurídico. Los origines del concepto de privacidad en el derecho anglosajón pueden encontrarse a nivel lingüístico en el dicho *the home is one´s castle* (el hogar es el castillo (del propietario)), que a su vez fue reconocido en la jurisprudencia inglesa en el caso *Semayne*[1]. [2]

[1] (77 Eng. Rep. 194 (K.B. 1604).

[2] Para un análisis más detallado del desarrollo legislativo de la privacidad en Estados Unidos ver: (Solove D. J., 2006)

En el derecho francés la *Loi Relative a la Presse* de 11 de mayo de 1868 establecía en su artículo 11 una prohibición a la publicación de actos relativos a la vida privada.

La importancia del aporte de Warren y Brandeis, quienes fueron motivados por publicación de información de la vida privada de Warren y su esposa, radica en la creación de una estructura jurídica coherente tras el análisis de varias decisiones judiciales en los Estados Unidos.[3]

Independientemente del motivo que hayan tenido los autores, la privacidad surge como respuesta a las limitaciones de la responsabilidad por difamación en el derecho anglosajón, el cual surge como una herramienta política del estado contra disidentes y que fue evolucionando hasta convertirse en un derecho privado (Rodriguez Samudio, 2014). Las acciones por difamación se limitan a información falsa que lesione la posición social del individuo, por lo que su aplicación no resulta coherente en el caso de que la información sea verídica, aun cuando la misma pueda afectar la honra o el estado emocional de un individuo.

En su análisis, Warren y Brandeis llegan a la conclusión de que herramientas legales establecidas, como lo son el derecho de autor, la difamación o el incumplimiento contractual no se adaptan plenamente al derecho de privacidad como lo reconoce la jurisprudencia de la época. La infracción a la vida privada de un individuo es, por naturaleza, una relación extracontractual, y no depende de algún tipo de protección jurídica especial.

La naturaleza jurídica del daño sufrido resulta de particular importancia, ya que la misma no protege derechos patrimoniales. El bien jurídico protegido mediante el derecho a la privacidad bajo la concepción Warren-Brandeis, el derecho a ser dejado en paz, es un derecho no patrimonial. Sin embargo, este derecho no le otorga a su titular la propiedad de la información ni del medio que la contenga. En este último caso, tanto la Warren y Brandeis como la jurisprudencia norteamericana reconocen que es posible transferir la propiedad sobre el medio físico donde se encuentra la información, por ejemplo, una foto, sin que el nuevo propietario tenga el derecho publicar la misma sin el consentimiento del titular de la información.

Es el control sobre la información, en específico el derecho a oponerse a la publicación de la misma, una de las características de la teoría clásica de la privacidad. No obstante, este derecho no les asiste a las figuras públicas en lo relativo a actos realizados en el ejercicio de sus funciones. Pero si sobre aquellos actos que no guarden relación con su cargo o con su capacidad para desempeñarse en el mismo.

En cuanto al derecho a la privacidad de los particulares Warren y Brandeis reconocen los siguientes límites:

1. No se protege información personal de interés público.
2. El derecho a la privacidad no protege información de carácter privado cuando la misma sea transmitida en circunstancias que otorguen una defensa bajo las reglas de difamación.
3. No se protege información transmitida de manera oral, salvo que exista un daño especial (*special damages*).[4]
4. El derecho a la privacidad se extingue cuando el interesado publica la información, o esta se publica con su consentimiento.
5. La veracidad de los datos no es una defensa en casos de violaciones al derecho de privacidad.

Sin embargo, la y a pesar de la influencia que las teorías de Warren y Brandeis ejercieron en el pensamiento jurídico estadounidense, las cortes optaron por una postura más conservadora en un primer momento. En 1902, la Corte de Apelaciones del Estado de Nueva York negó la pretensión de daños y perjuicios en un caso donde la compañía demandada había utilizado una litografía de la demandada sin obtener su consentimiento. [5] La Corte fundamento su opinión en el hecho que no

[3] La responsabilidad extracontractual en el derecho anglosajón no sigue la figura continental europea de una cláusula general, siendo desarrollada mediante diversas pretensiones denominadas *Torts,* cada uno de los cuales tiene sus características particulares, las cuales deben ser probadas en el juicio. De allí la importancia del artículo de Warren y Brandeis, ellos fueron capaces de reconocer el desarrollo temprano de un nuevo *Tort*, y trataron de sistematizarlo y definirlo a fin de lograr su reconocimiento.

[4] El término *special damages* se utiliza para referirse a perjuicios económicos derivados de la publicación de la información.

[5] Roberson v. Rochester Folding Box Co., 64 N.E. 442 (N.Y. 1902).

existía un precedente claro, por lo que no le correspondía a la corte abrogarse funciones legislativas mediante la creación de una clase de acción judicial. La respuesta a este fallo fue inmediata, y en 1903 el órgano legislativo del estado de Nueva York aprobó una ley prohibiendo la invasión a la privacidad. No fue hasta 1905, con el caso *Pavesich v. New England Life Insurance Co*.[6] en el que una corte estadounidense, en este caso la Corte Suprema del estado de Georgia, reconoce por primera vez el derecho a la privacidad. La corte no fundamentó su decisión en la existencia de una ley en particular, considerando que el derecho a la privacidad que emana del derecho natural.

Por otra parte, los límites de la teoría clásica del derecho a la privacidad, basada en un control sobre la publicación fundamentada en la naturaleza no patrimonial del bien jurídico protegido, comienzan a hacerse evidentes para la década de los años 50. Nuevamente, el desarrollo de nuevas tecnologías, en este caso la televisión y el cine, pusieron en entredicho las bondades de un enfocado en limitar el uso indebido de información personal. Nimmer (Nimmer, 1954) argumenta que personalidades públicas, en particular celebridades de cine, han descubierto maneras de beneficiarse económicamente de su imagen y nombre, a una escala jamás vista hasta entonces.

La crítica de Nimmer no se centra en argumentos ontológicos, morales o de orden público, sino que se enfoca en un la situación particular de actores, deportistas y otra figuras públicas, quienes, producto de su fama, no pueden reclamar beneficios por el uso de imagen.[7] En específico, Nimmer se enfoca en la naturaleza intransferible del derecho a la privacidad, y argumenta que el derecho de publicidad es un derecho real por lo que su titular puede asignarlo a un tercero, y este a su vez puede hacerlo valer cuando tal derecho resulte violentado.[8] Esto contrasta con la naturaleza jurídica de la privacidad bajo la estructura Warren-Brandeis, bajo la cual la privacidad es un derecho personal, cuya infracción no debe considerarse como un daño pecuniario, sino como un ataque a la esfera de los intereses no económicos del individuo. No obstante, y a pesar de que el argumento de Nimmer hace extenso uso de celebridades tanto humanas como no humanas[9], el mismo reconoce que no existe un fundamento para limitar su aplicación únicamente a personas que hayan obtenido el estatus de celebridad, pero que el monto de cualquier indemnización dependerá en gran medida de la fama del demandante.

Si bien no tan influyente como el artículo de Warren y Brandeis, la teoría propuesta por Nimmer resulta importante para los objetos de este estudio por dos razones. La primera es que abrió la puerta a las discusiones sobre el derecho a la publicidad, industria millonaria hoy en día. La segunda es que el argumento presentado por Nimmer puede considerarse como una de las primeras teorías jurídicas que utilizan el concepto de un beneficio particular producto del uso datos personales, aunque en un sentido sumamente restringido.

El Estado y el concepto de privacidad

La doctrina jurídica sobre privacidad hasta mediados del siglo XX se fundamenta en conceptos eminentemente anglosajones. Esto no implica que otros países no hayan abordado el tema hasta la introducción las teorías de Warren y Brandeis. Por el contrario, muchos países del sistema continental europeo, en particular aquellos con un sistema de responsabilidad extracontractual de clausula general, ofrecían un cierto grado de protección a la dignidad del individuo. No es hasta culminada la segunda guerra mundial, con la Declaración Universal de los Derechos Humanos de la ONU de 1948, que la privacidad inicia un proceso de internacionalización.[10] Los inicios de la segunda mitad del siglo XX ven el desarrollo de una nueva vertiente doctrinal de la privacidad,

[6] Pavesich v. New England Life Ins. Co., 50 S.E. 68 (Ga. 1905).
[7] Ibíd.
[8] Ibíd. p.216.
[9] Nimmer pone como ejemplo el famoso perro Lassie para explicar la limitación de la privacidad como un derecho inherente a los seres humanos implica que el uso comercial de su imagen o nombre sin permiso de sus dueños no le otorga a sus dueños, o al estudio, ningún tipo de remedio para recuperar perjuicios sufridos. Ibíd. p.210.
[10] El artículo 12 de la Declaración Universal de los Derecho Humanos establece que "Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques".

aquella que otorga un gran énfasis al rol del Estado en la recolección y protección de la información de sus ciudadanos.

Tras las labores de reconstrucción en Europa, los estados europeos se vuelcan a la tarea de fortalecer sus instituciones jurídico-políticas, primero mediante la creación de organismos de cooperación económica como la Comunidad Económica Europea, que eventualmente concluyen con la creación de la Unión Europea. Como parte de estos esfuerzos, inician discusiones sobre la importancia del concepto de privacidad como parte de la dignidad del individuo.

Este último punto es uno de los elementos distintivos más importantes entre los sistemas de protección de datos personales en occidente. Whitman (2004) considera que la diferencia fundamental entre los dos sistemas occidentales de privacidad, el estadounidense y el europeo, radican en fundamentos sociales y políticos.

En particular, las tecnologías de recolección de datos desarrolladas durante la segunda guerra mundial contribuyen enormemente a que la discusión sobre privacidad se traslade de la publicación de los datos a su recolección y uso. Sin embargo, durante esta época, y a diferencia de la situación actual, las tecnologías de recolección y análisis de información solo son accesibles a actores e instituciones estatales, por lo que el Estado adquiere un rol protagónico en la evolución del concepto de privacidad. En particular, la doctrina del Macartismo impulsada por el senador estadounidense Joseph McCarthy de 1950 a 1956, puso de manifiesto la necesidad de límites al poder estatal en lo que se refiere a la recolección y uso de la información de sus ciudadanos so pretexto de la seguridad nacional.

Por una parte, el alto costo de estos equipos implica que su acceso se vea restringido a entes gubernamentales y que su uso sea para fines administrativos o de seguridad. Por otra parte, para ese momento el concepto de privacidad había cambiado a tal punto que resultaba difícil encontrar una teoría unitaria sobre el tema ampliamente aceptado. Esta situación impidió en cierta manera el desarrollo de legislaciones que regularan la materia. Por ejemplo, en Inglaterra el Comité Younger sobre Privacidad recomendó en 1972 no legislar sobre el tema ante la falta de consenso sobre el contenido y límites del derecho a la privacidad (Solove D. J., 2008).

Tal es la importancia y preocupación que despierta el poder estatal de recolección de información que el mismo fue el tema central de la primera legislación mundial sobre privacidad. La *Datalegen* sueca de 1973 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 (Öman, 2004).[11]

En 1973, el Departamento de Salud, Educación y Servicios Sociales de los Estados Unidos, elabora un informe donde recomienda la adopción de un Código de Practicas de Información (U.S. Department of Health, Education & Wellfare, 1973). El reporte reconocía 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. En sus recomendaciones, el reporte establece una serie de principios generales que deben gobernar la recolección y manejo de datos:

1. No deben existir registros de datos secretos.
2. El titular debe tener un método para conocer qué información se ha recopilado y que uso se le da.
3. Debe existir un mecanismo para que el titular impida el uso de su información de manera distinta por la cual se recolecto.
4. Establecer un método para el titular pueda corregir información errónea.
5. La organización que creé mantenga, utilice o distribuya la información debe asegurar su uso correcto para el fin establecido.

En 1974 se promulga en Estados Unidos la Privacy Act que regula la recolección y protección de datos por parte de agencias estatales. Sin embargo, su aplicación se limita a ciudadanos

[11] (Öman, 2004, p. 390)

estadounidenses o extranjeros que residan legalmente de manera permanente en Estados Unidos.[12] Las recomendaciones del reporte del el Departamento de Salud, Educación y Servicios Sociales de los Estados Unidos, en particular los principios recogidos en su Código de Practicas Informativas sirvieron como base para la creación de las *Guidelines on the Protection Of Privacy and Transborders Flows of Personal Data* adoptados por la OECD en 1980 y que fueron actualizadas por última vez en 2013.

Estas guías, junto con la Convención para la Protección de los Individuos en lo Relativo al Procesamiento Automático De Información Personal, también conocido como el Tratado 108 del Consejo Europeo, fueron el fundamento del derecho a la privacidad a nivel europeo hasta la creación de la Directiva de Protección de Datos (Directiva 95/46/EC) en 1995. Tanto las guías de la OECD como el Tratado 108 establecen los principios de aviso previo y consentimiento informado, determinación del uso de la información, prevención de acceso indebido, el derecho del individuo a conocer que datos han sido recolectados, el derecho al acceso a dichos datos, el derecho a cuestionar la necesidad del almacenaje de los datos y el derecho a requerir su corrección o eliminación.

A nivel de derecho anglosajón surge el concepto de la expectativa de privacidad (*expectation of privacy*). Originalmente planteada en el caso de Katz v. United States[13], esta doctrina es otro control sobre el poder del Estado, en particular sobre las facultades investigativas de entes estatales como la policía, en lugares públicos. Fundamentada en la cuarta enmienda a la Constitución estadounidense, este estándar prohíbe pesquisas e investigaciones en lugares públicos en los cuales el individuo tenga una expectativa de privacidad. En Inglaterra y otros países del Reino Unido, así como en países pertenecientes a la Mancomunidad de Naciones (*Commonwealth*), la doctrina se conoce como expectativa razonable de privacidad (*reasonable expectation of privacy*).

Por otro lado, la leyes de privacidad en materia de responsabilidad civil entre particulares también continuaron avanzando. El jurista William Prosser (1960), tras un análisis exhaustivo de la jurisprudencia estadounidense, pudo establecer que el derecho de la privacidad había evolucionado para incluir cuatro tipos de reclamaciones.

La primera es la intrusión del aislamiento del individuo (*intrusión upon seclusion*), la cual es una intromisión altamente ofensiva, en base al estándar de una persona razonable, en la vida privada de un individuo. Este tipo de reclamos incluye, tanto fotografías, violación al secreto, invasión a la privacidad en la residencia e inclusive nuevas tecnologías de la época como conversaciones de teléfono privadas.

El segundo tipo de violaciones es la divulgación publica de información privada (*public disclosure of private facts*), que no es más que la teoría tradicional de la privacidad. La diferencia con la intrusión al aislamiento radica en que aquel caso el daño se causa por la recolección de la información, mientras que en el caso de la divulgación la información privada puede haber sido obtenida de manera legal, por ejemplo haber recibido una carta bajo un contrato de depósito, pero el poseedor de la información no puede divulgarla.

El tercer tipo de infracción es la falsa imagen (*false light*) que no es mas que la divulgación publica de información que cause que el titular de la misma se vea afectado negativamente en su imagen. Cabe destacar que la información debe ser verdadera, de lo contrario estaríamos hablando de difamación. La violación al bien jurídico consiste en la publicación de información que, siendo verdadera, cause que el individuo un cierto nivel de honra o estatus social, o bien sea objetos de otro tipo de perjuicios económicos o no. Un ejemplo claro puede ser la publicación relativa a la homosexualidad de un individuo en una comunidad altamente religiosa. Finalmente, la última infracción reconocida es la apropiación (*appropiation*), la cual consiste en el uso indebido de la imagen o nombre de otra persona para beneficio propio.

El aporte más importante en materia de doctrina jurídica durante esta época es la creación de un sistema basado en los conceptos de aviso previo y consentimiento informado. El individuo, ya no

---

[12] En enero de 2017, mediante orden ejecutiva, el presidente Trump ordenó a las agencias bajo su mando excluir de la protección de datos a aquellos individuos que no residan legalmente en Estados Unidos. https://www.whitehouse.gov/presidential-actions/executive-order-enhancing-public-safety-interior-united-states/
Fecha de consulta: 16 de agosto de 2019.

[13] Katz v. United States, 389 U.S. 347

como particular, sino en base a su calidad de nacional de un estado o, fundamentado en un derecho natural, tiene el derecho a conocer quien recolecta su información, para que fin, y que información está siendo recolectada. La introducción de este modelo constituye un cambio radical en el pensamiento jurídico de los derechos del individuo en lo relativo a su información personal. Ya no puede hablarse de un Estado con poder absoluto para requerir o recolectar la información personal de sus ciudadanos de manera secreta. Se imponen nuevas reglas de conducta, y cambia la percepción de los límites del poder estatal en lo referente a la administración de la información pública.

La privacidad en los inicios de la era digital

Para finales de la década de los 80 y principios de los 90, la introducción de computadores personales de uso doméstico dio como resultado una expansión acelerada del uso de información en la sociedad en general. A las discusiones sobre los poderes y responsabilidades de los organismos estatales en el manejo de la información se añaden la preocupación sobre la recolección y uso de información por parte de organizaciones particulares.

De igual manera, las discusiones sobre el concepto de privacidad continúan sin que pueda encontrarse un consenso. Las preocupaciones sobre la divulgación de información se conjugan con preocupaciones practicas sobre la obtención de esta, atrás quedan los tiempos donde la existencia de una carta o documento se limitaba a su existencia física o de una copia. Con la introducción de servicios de email y mensajería instantánea durante la década de los 90 la información deja de ser local y se inicia una globalización de las comunicaciones.

El papel de la información en este nuevo mundo tecnológico significa que las controversias privacidad ya no puede limitarse al esquema de publicación de información Warren-Brandeis, ni a la recolección por parte

Las normas europeas relativas a privacidad comienzas a dejar su marca a nivel internacional. La razón de esto puede atribuirse a dos fenómenos puntuales. El primero es la integración europea alcanzada durante la segunda mitad del siglo XX, lo cual implica una uniformidad en la letra, espíritu y aplicación de las normas europeas. El poder económico del bloque europeo se traduce en un mayor poder negociación frente a estados unidos, lo que permite el desarrollo de nuevos estándares en diversas ramas. El segundo fenómeno que influye en la transformación del concepto de privacidad es la eliminación de barreras físicas de almacenaje de datos y la explosión en el desarrollo de tecnologías de la comunicación.

En particular, el uso de computadores personales y cuentas de email significa que la información puede transmitirse instantáneamente, creando o conservando un número casi ilimitado de copias. La información de un individuo ya no se reduce a medios físicos, ni se encuentra atrapada dentro de los límites geográficos de un Estado. Aunado a esto, la globalización permite a las empresas conservar información de sus clientes independientemente del lugar donde la transacción se haya perfeccionado.

En respuesta a estas nuevas realidades, la Unión Europea aprueba la Directiva de Protección de Datos (Directiva 95/46/EC) en 1995, norma que se convertirá en el norte del derecho a la privacidad a nivel europeo hasta 2016. En cuanto al contenido, la Directiva 95/46/EC expande los principios de las guías de la OECD y el Tratado 108 del Consejo de Europa.

La primera mitad de la década de los años 90 no produjo nuevas doctrinas jurídicas relativas a la privacidad, concentrándose mayormente en la aplicación y adaptación de las reglas desarrolladas durante los años 70 y 80. En cierta medida, los avances tecnológicos no fueron tan disruptivos como aquellos que les precedieron. Es con el aumento de tecnologías digitales de uso personal durante la segunda parte de la década que inician nuevas discusiones sobre el control de los datos personales.

Transformaciones en la era digital.

El boom del *dot com,* en el cual miles de compañías online fueron fundadas en un corto periodo de tiempo, solo para crear una crisis económica cuando la mayoría de ellas se dieron a la quiebra a finales del siglo XX principios del siglo XXI también demostró la disposición de los individuos

particulares de proporcionar información personal a cambio de un beneficio tangible. Sin embargo, este intercambio no puede concebirse bajo la misma premisa del derecho a la publicidad, ya que la información proporcionada por cada individuo tiene un valor propio, independientemente de la fama que del titular. De allí, que el valor de la información se su calidad como información y de la cantidad que pueda ser recolectada.
En la época de Warren-Brandeis la privacidad era un concepto personal, un derecho a no ser molestado en aquellos asuntos de la esfera íntima del individuo. La violación de tal derecho se limitaba a la publicación de tal información, aunque la misma hubiese sido obtenida de forma licita. En ese momento la información personal no tenía ningún valor y la publicación de conversaciones privadas o fotografías no representaba más que un acto tendiente a causar un sufrimiento emocional al titular o para presionarlo a tomar una determinada decisión.

Con el uso de tecnologías digitales comienzan discusiones sobre la naturaleza jurídica de la información, en particular, la posibilidad de ejercer un derecho de propiedad sobre la información personal.

Esto se hace evidente con la aparición de las primeras redes sociales a mediados de la primera década del siglo XXI. La discusión sobre el valor y la propiedad de la información en las diversas plataformas de servicios digitales continúan hoy en día. Los países europeos, guiados por los principios de dignidad expuestos anteriormente, han optado por una mayor protección de la información de sus ciudadanos. El ejemplo más claro de esto es el nuevo Reglamento General de Protección de Datos (RGPD) de 2016, que fija los nuevos principios rectores en materia de protección de datos personales a nivel europeo. En cambio, el modelo estadounidense, guiado quizás por el hecho de que mayoría de las innovaciones tecnológicas han surgido de compañías de ese país, opta por dar mayor importancia a la innovación tecnológica. Las normas relativas a la privacidad se adaptan a la tecnología no en base a una actualización legal, sino a la aplicación por analogía con fundamento al amplio alcance del texto legal.

Por otro lado, los ataques terroristas del 11 de septiembre de 2001 en Estados Unidos reavivan las discusiones sobre la necesidad de una vigilancia constante so pretexto de la seguridad nacional. Este fantasma del Macartismo, constituya una sombra sobre la manera en que la relación ciudadano-Estado debe entenderse en el nuevo milenio.

Taxonomía de la privacidad en la era digital

De la misma manera que Posner, Solove (2006) realiza un análisis de las maneras en las que la privacidad de un individuo puede ser afectada mediante el uso de nuevas tecnologías digitales. Esta taxonomía reconoce cuatro tipos de actividades que hacen uso de la información personal en el nuevo milenio: 1. Recolección de información, 2. Procesamiento de la información, 3. Diseminación de la información, y 4. Invasión.

La categoría de recolección de la información se subdivide en vigilancia e interrogatorios. Esto es consonó con los principios generales de control de información, en particular el principio de aviso previo y consentimiento informado, ya que solo la recolección de información sin el consentimiento del titular puede considerarse como un ataque a la privacidad.

El procesamiento de la información consiste en la agregación, identificación, inseguridad, utilización secundaria y exclusión. Agregación es el proceso de recolección de información personal de un individuo que, por si sola, no ofrece muchos detalles sobre el titular pero que en conjunto puede revelar información sensitiva. El problema de la identificación puede resumirse en el vínculo entre la información y el titular. La identificación en si no se configura en una infracción a la privacidad del individuo, sin embargo, en algunos casos la información puede producir efectos adversos a la honra o estatus social del titular.

La inseguridad guarda relación tanto con la agregación como con la edificación. Una estructura informática con sistemas de protección deficientes pone en riesgo la información almacenada. Con acceso a esta información es posible copiar la identidad de un individuo, obteniendo acceso a datos bancarios, etc. La utilización secundaria se refiere al uso de los datos recolectados en una manera no cónsona con el aviso previo dado al titular al momento de la obtención su consentimiento. Por último, la exclusión se da cuando los sistemas de bases de datos

no informan al titular que su información está siendo almacenada, lo que deriva en problemas al momento de exigir rendición de cuentas.

La diseminación de la información abarca problemas comunes relativos al uso de información que, sin ser exclusivos a las tecnologías digitales, se ven exacerbados mediante el uso de estas. Actos como violación a la confidencialidad, divulgación de datos privados, revelación de características físicas o emocionales, aumento al acceso a la información, extorsión, apropiación de la información o distorsión de los hechos son ejemplos de esta categoría.

Finalmente, la categoría de invasión contempla dos conductas puntuales. La intrusión, que es la invasión de la vida personal del individuo, alterando sus actividades diarias, rutinas cotidianas, violentando su derecho a la soledad y causándole estrés y molestias. Por lo general son conductas que constituyen acoso, es decir una violación intrusión prolongada de la privacidad de la víctima. La otra conducta constitutiva de invasión es la interferencia en la toma decisiones, que se da cuando la posibilidad de que cierta información sea divulgada al público afecta la decisiones del individuo. Un ejemplo de esto puede ser información médica sobre ciertos tratamientos, por ejemplo enfermedades de transmisión sexual, métodos anticonceptivos, etc., los cuales, pueden afectar el estatus social del paciente si se llegará a divulgar el hecho de que ha sido objeto de estos tratamientos.

El futuro de la privacidad en la era de ciudades inteligentes

La taxonomía presentada por Solove fue diseñada bajo los principios rectores del derecho a la privacidad, en particular el concepto de consentimiento informado a partir de un aviso previo. Este esquema tenía como punto de partida la idea de que las nuevas tecnologías estarían basadas en plataformas de software, con un cierto nivel de integración a servicios en línea. Sin embargo, los avances tecnológicos de la última década se han enfocado en el uso de la información como materia prima para la creación de nuevos productos y servicios.

Si bien es cierto que en la actualidad muchos de estos servicios de redes sociales hacen amplio uso de los datos personales de sus usuarios con fines mercadotécnicos, de publicidad y en algunos casos para estudios científicos, estos servicios se basan en un consentimiento por parte del usuario, aun cuando en muchos casos sus políticas de privacidad no sean lo suficientemente claras para que dicho consentimiento pueda considerarse informado.

En cambio, el nuevo desafío en materia de privacidad no se encuentra en estas plataformas en líneas, sino en la creación de ciudades inteligentes. Actualmente, no existe un concepto único de lo que puede considerarse una ciudad inteligente. Sin embargo, existen una serie de características comunes que las distinguen.

Kitchin (2015) explica que una ciudad puede ser llamada inteligente si se enmarca dentro de uno de los siguientes modelos. Bajo el primer modelo de ciudad inteligente, los ciudadanos adoptan medidas de gobierno en base a los datos recolectados. El segundo modelo define una ciudad inteligente como aquella que hace uso de la tecnología para mejorar las regulaciones y políticas urbanas mediante la reconfiguración del capital humano, con el fin de mejorar elementos como la educación, innovación, creatividad, sostenibilidad y gestión. Finalmente, el tercer modelo propone que una ciudad puede considerarse inteligente en la medida que utilice tecnologías de información para desarrollar iniciativas sociales, justicia social, activismo, transparencia y responsabilidad gubernamental.

Edwards (2016) explica que el mayor desafío que presentan las ciudades inteligentes en materia de privacidad es el uso de tecnologías como el internet de las cosas, procesamiento de macro datos y computación en la nube. El internet de las cosas implica una conexión constante al internet de productos que normalmente no harían uso de este servicio, como refrigeradoras, camas, etc. Estos productos recogen información del usuario para ofrecer un servicio personalizado. Sin embargo, y debido a que por su naturaleza estos productos suelen ser de fácil uso, no suelen contar con los mecanismos tradicionales para la correcta recolección de la información. Por ejemplo, los relojes Smart y bandas de salud no le presentan al usuario las políticas de privacidad en la pantalla, en la mayoría de los casos siendo necesario que el usuario las consulte mediante otro dispositivo.

La información recolectada mediante dispositivos que utilicen el internet de las cosas puede ser procesada mediante algoritmos de macro datos y almacenada en línea mediante tecnologías de la nube, lo que permite un mayor poder de procesamiento y un acceso a nivel global.

Diversas industrias han encontrado usos para la información recolectada, ya sea como materia prima o tras su procesamiento. Esto implica que a diferencia de los tiempos de Warren y Brandeis, la información en si tenga un valor pecuniario, si bien el mismo resulta ínfimo cuando hablamos de los datos de un solo individuo. Esto ha reavivado las discusiones sobre un derecho de propiedad sobre la información. Los promotores de este derecho argumentan que es posible reconocer la propiedad de la información al momento de la creación y establecer mecanismos para ejercer los derechos, privilegios, controles y limitaciones sobre la información de manera que permita su uso mediante plataformas de contratos electrónicos (Ritter & Mayer, 2016).

Por otra parte, detractores de un derecho a la propiedad sobre la información argumentan que la creación de tal derecho no es adecuado para promover la privacidad o avances tecnológicos. Por el contrario, un derecho a la propiedad sobre la información se traduciría en una limitante a la libertad de expresión, libertad de información, a la ciencia y al progreso tecnológico. (Determan, 2018)

Conclusiones

La privacidad ha evolucionado a lo largo de sus más de 100 años de historia como un derecho individual. Este proceso se ve marcado por la gran influencia que ejercen las tecnologías sobe el concepto de lo que puede considerarse privado. En cierta medida, la fluidez conceptual de la privacidad ha contribuido a que su alcance sea difícil de comprender. Esto es por cuanto, la privacidad, en su proceso transformativo, no suele rechazar ideas previas, ni cambiar su discurso, sino que incorpora las nuevas teorías a su marco conceptual.

Esta flexibilidad se constituye tanto en la mayor fortaleza como en la el talón de Aquiles de las doctrinas de privacidad modernas que, al igual que cualquier otra rama del derecho, siempre estará un paso atrás del desarrollo de nuevas normas sociales y tecnológicas. Sin embargo, en esta ocasión el salto tecnológico puede ser más grande de lo que se esperaba. La información personal, aun cuando la misma ha sido anonimizada, ha adquirido un valor pecuniario. Ya no es posible limitar el análisis a la protección de la honra o de la libertad del titular de la información, sino que se hace necesario replantear el papel del individuo frente a los beneficios que recibe a cambio de sus datos.

Si el futuro del desarrollo humano ha de centrarse en centros urbanos inteligentes, la dinámica privacidad-innovación-control debe ser el objeto central de futuras discusiones sobre el tema.

BIBLIOGRAFÍA

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

Determan, L. (2018). No One Owns Data. *Hastings Law Journal, 70*, 1-44.

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

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

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.

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.

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

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

Prosser, W. L. (1960). Privacy. *California Law Review, 48*(383-423).

Ritter, J., & Mayer, A. (2016). Regulating data as property: a new construct for moving forward. *Duke Law and Technology Review, 16*(1), 221-277.

Rodriguez Samudio, R. E. (2014). El daño no económico en el derecho estadounidense. *Revista Facultad de Derecho y Ciencias Políticas, 44*(121), 609-644.

Solove, D. J. (2006). A brief history of information privacy law. En *Proskauer on Privacy.* PLI.

Solove, D. J. (2006). A taxonomy of privacy. *University of Pensilvania Law Review, 154*, 477-560.

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

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.

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

Datos del autor:

Doctor en Derecho, Universidad de Hokkaido, Japón.
Profesor asistente de la Universidad de Hokkaido, Japón.
Abogado de la República de Panamá.
Correo electrónico: rubenr1618@gmail.com, ruben18@juris.hokudai.ac.jp

Artículo recibido: 14 de septiembre de 2019

Aprobado: 26 de septiembre de 2019