Tesina para la Escuela de Derecho de la Universidad de Valparaíso

El Internet de las Cosas ¿Una amenaza al Derecho a la Privacidad?

Autores:
Celeste Gajardo
Kevin Munizaga

Profesora guía:
Patricia Reyes Olmedo

Diciembre 2022

ÍNDICE

Tabla de Abreviaturas

IoT	Internet of Things.
OCDE	Organización para la Cooperación y el Desarrollo Económico.
Derechos ARCO	Derechos de Acceso, Rectificación, Cancelación y Oposición.
Derechos ARCOPI	Derechos de Acceso, Rectificación, Cancelación, Oposición, Portabilidad e Impugnación
UE	Unión Europea.
RGDP	Reglamento General de Protección de Datos.
CE	Constitución Española
LOPDGDD	Ley Orgánica de Protección de Datos y Garantía de los Derechos Digitales.
DG Connect	Dirección General de Sociedad de la Información y Medios de Comunicación.
NIST	Instituto Nacional de Estándares y Tecnología

Resumen

El presente texto se enfocará en abordar en cómo el creciente avance de las tecnologías y el Internet de las cosas no ha ido creciendo a la par de la legislación chilena, la que no ha tenido por prioridad la correcta regulación y aplicación de los derechos digitales, generando distintas vulneraciones a derechos fundamentales que nuestro ordenamiento consagra. Para abordar sistemáticamente debemos, en primer lugar, entender el derecho a la privacidad y al concepto del Internet de las cosas; en segundo lugar, se analizará la Ley N° 19.628 sobre la protección de los datos personales y el proyecto de ley que se tiene en tramitación para su modificación; en tercer lugar, de casos históricos que se registran en Chile; cuarto lugar, un estudio sobre derecho comparado de la Unión Europea y Estados unidos; por último, nuestra propuesta de aplicación y regulación que en Chile debería regir.

Palabras clave: Internet de las Cosas- Derecho a la privacidad- Datos personales-Ley 19.628- Regulación europea al IoT

Introducción

Desde finales del siglo pasado se ha ido desarrollando una nueva tecnología que poco a poco ha ido conectando el mundo, hablamos de Internet, el cual data de la mitad del siglo XX, naciendo de la necesidad de interconectar las computadoras que en ese entonces se utilizaban para guardar archivos gubernamentales en los países más desarrollados del mundo. Internet fue evolucionando junto con las mismas computadoras, siendo a finales de los años 90´ el comienzo de su distribución al público en general, naciendo con esto un nuevo tipo, el llamado Internet de las Cosas (IoT de ahora en adelante por sus siglas en inglés), siendo hoy en día una parte fundamental para la vida de las personas en todo el mundo y también para nuestro país, calculándose que la inversión en Chile del IoT en 2021 según la EAE Business School superó el 5.5% de nuestro PIB anual, siendo el 4to país de América Latina que más gastó en esta tecnología durante 2022. Otro dato importante para considerar es el ranking latinoamericano de ciudades inteligentes *Cities in Motion Index*, en el cual Santiago de Chile paso de comenzar a apostar recién por el modelo en el año 2018, a liderar el ranking en Latinoamérica en 2020, obteniendo el puesto número 68 mundial (Gallego, 2022: pp. 21-23)

Está tecnología permite solucionar diferentes problemas y monitorear diversos aspectos de nuestra vida, un ejemplo de ello podría ser la utilización de un refrigerador inteligente para monitorear el estado de los alimentos o determinar cuáles son los que están faltando para una alimentación saludable, relojes inteligentes que cuentan cuántos pasos estamos dando en nuestro día a día, incluso sistemas que ven cual es nuestro comportamiento al dormir o al manejar un automóvil para determinar qué póliza de seguro es la adecuada, hasta ejemplos que van más allá del ámbito del hogar o el individuo, ya que hoy en día existen redes de ciudades denominadas inteligentes, las cuales buscan optimizar diversos asuntos en búsqueda de una mejor sostenibilidad con el medio ambiente. Todos estos ejemplos nos hacen ver que estamos insertados en un sistema global interconectado, dependiente del Internet en todo momento y de su nube que almacena además información de nuestro diario vivir, el cual podríamos pensar que ese futuro que los habitantes de principios de siglo XX con todas las facilidades que esto conlleva, aun no llega del todo, pero realmente el futuro digital es hoy. Sin embargo, tal como

dice Cortez en 2014 “el IoT ¿Ya es algo realmente distinto a lo que tenemos? ¿Este IoT conlleva algunos riesgos en nuestra vida?”(Cortez, 2014: p. 3)

Estos riesgos son los que nos lleva a hacer un estudio sobre el panorama del IoT en nuestro país y los diversos problemas que implica, siendo el más importante las afectaciones al derecho a la privacidad, ya que durante los últimos años se han incrementado los dispositivos conectados al IoT, los que recopilan innumerables tipos de datos sobre su utilización, como por ejemplo tiempo de uso, intereses y preferencias de los usuarios, los que luego son utilizados para sacar réditos económicos, políticos, pues son vendidos con fines distintos a los que se recopilan. Lo anterior, nos hace preguntarnos si en verdad se respeta la privacidad de las personas y su consentimiento con esta desmedida, y en muchos casos maliciosa, recopilación de estos datos. Finalmente, el trabajo también se enfoca en analizar la regulación que existe en nuestro país sobre el derecho a la privacidad para compararla con la regulación de países como el Reino Unido y Estados Unidos, proponiendo algunas directrices para un modelo de mejor regulación en nuestro país.

Capítulo I: El Internet de las cosas y la privacidad

1. Derecho a la privacidad

1.1. Concepto

El Derecho a la privacidad desde los inicios de la humanidad ha sido inherente a los hombres, el solo hecho de no querer que una persona ajena se entrometa en nuestra vida es parte importante para poder desarrollar ciertas áreas de nuestra personalidad. El desarrollo de este derecho hace difícil encontrar un solo concepto unitario, ya que este dependiendo del punto de vista del que se mire es posible encontrar diferentes conceptos, por ejemplo, uno de los primeros conceptos que se dieron de este derecho, en el ámbito que nos ocupa, es la frase que citaron Warren y Brandeis en 1890 ante el juez Cooley, "el derecho a estar solo"(Herrera, 2016: p. 88), el cual se asociaba al derecho que tenían las personas a no sufrir una intromisión de la prensa o de un tercero ajeno a su vida privada. Esta definición es el punto de partida de la consolidación de la privacidad como un derecho fundamental.

A mitad del siglo pasado, se inauguraría otro concepto del derecho a privacidad, fue gracias a la Corte Suprema de Estados Unidos. Al respecto, Corral dice que "esta fue la que inauguró la visión de que el derecho a la vida privada, en última instancia, significaba el derecho a adoptar libre de injerencias ajenas decisiones que afectaran a la vida personal, Esta es la línea de razonamiento que se vislumbra en el caso Griswold (1965), Eisenstadt (1972) y se ratifica en Roe (1973)" (Corral, 2000: p. 335), por lo que de solo no permitir injerencias pasamos a que las personas tengan una especie de control sobre sus decisiones personales y que estas no sean afectadas por terceros ni sean observadas por estos.

1.2. Interpretación del derecho a la privacidad

Este punto de control que definíamos anteriormente ha traído problemas en la jurisprudencia y la doctrina, ya que como menciona Herrera, ambas "tienen una difícil tarea

de esclarecer, por una parte, cuando una situación transgrede ¿la? privacidad de un individuo y, de otra, cuáles son los límites de lo público y lo privado"(Herrera, 2016: p. 89), por lo mismo, sería contraproducente decir que el derecho a la privacidad es algo absoluto, porque se encuentra con la vida pública, por lo que hay que buscar límites para que ambos espacios, el público y el privado, no colisionen, un ejemplo de esto es que lo que dice el mismo autor respecto a que con todas las tecnologías nuevas que han salido se ha aumentado la dificultad de delimitar estos territorios(Herrera, 2016), un ejemplo de esto lo podemos observar en una conversación que hoy en día puede tener una persona por teléfono en la vía pública la que puede ser igual de privada que lo que hagamos en nuestros hogares.

1.3. Regulación

Debemos de partir mencionando que el derecho a privacidad está fuertemente regulado en el derecho internacional en el artículo 12 de la Declaración Universal de los Derechos Humanos, siendo reafirmado posteriormente en el artículo 17 del Pacto Internacional de Derechos Civiles y Políticos de 1966, estableciendo que nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y reputación. Nuestro país ratifico ambos tratados internacionales.

En nuestro país el derecho a la privacidad, o protección de la vida privada, está regulado primeramente por la Constitución, en el artículo 19 numeral 4 que asegura a todas las personas "el respeto y protección a la vida privada y a la honra de la persona y su familia, y, asimismo, la protección de sus datos personales". También en el numeral 5 que asegura la "inviolabilidad del hogar y de toda forma de comunicación privada" (CPR, 1980), esta regulación a nivel constitucional está protegida por el recurso de protección del artículo 20. Es importante también mencionar que en 2018 el articulo 19 numeral 4 anteriormente mencionado fue reformado por medio de la ley 21.096, el cual se le agregó la frase "asimismo, la protección de datos personales", consagrando constitucionalmente el derecho a la protección de datos personales, que estaba regulado anteriormente en la ley 19.628 promulgada en agosto de 1999. Esta reforma es un avance a la del derecho a privacidad en el ámbito de la protección de datos personales, sin embargo, llega muy tardíamente frente al

avance acelerado de las tecnologías, ya que entre la promulgación de la ley 19.628 y la ley 21.096 han pasado casi 19 años

2. El Internet de las cosas

2.1. Definición del IoT

Desde que se comenzó a dar un uso más cotidiano e intensivo al Internet a principios de la década de los 90, se ha buscado una mayor conectividad de la sociedad. Durante esta búsqueda, en 1999 Kevin Ashton, uno de los pioneros de esta nueva tecnología, en una presentación que hizo en "Procter & Gamble" fue el primero en utilizar el término "Internet of things"(Salazar and Silvestre, 2019: p. 7), esto buscando llamar la atención de su nueva tecnología de red RFID ("la cual es toda tecnología capaz de utilizar ondas de radio para identificar de forma automática tanto objetos como personas o animales"(Espejo, 2018: p. 3)). Pero ese no fue el inicio del IoT, recién a finales de la década del 2000, se dio nacimiento como tal al Internet de las cosas como hoy se conoce, y que "se refiere a los escenarios en los que la conectividad de red y la capacidad de cómputo se extienden a objetos, sensores y artículos de uso diario que habitualmente no se consideran computadoras, permitiendo que estos dispositivos generen, intercambien y consuman datos con una mínima intervención humana"(Rose, Eldridge and Chapin, 2015: p. 13).

2.2. Historia del IoT

El primer objeto conectado a Internet fue creado por John Romkey en 1990, era una tostadora que tenía la capacidad de encenderse y apagarse por medio remoto. A partir de ese hecho y con la llegada del nuevo milenio empezaron a aparecer más objetos conectados a Internet, como lo fue el refrigerador LG Internet Digital DIOS, que no tuvo éxito debido a su alto precio y que las personas lo vieron como un objeto innecesario, a consecuencia de que en esa época aún se veía a los computadores como el único medio para acceder a

Internet. Esto deja de ser así a partir de 2006, en que comienza el boom por los teléfonos inteligentes (teléfonos que hoy en día consideraríamos simplemente teléfonos convencionales con funciones). En esa época Nokia comienza a vender estos teléfonos "inteligentes" con un enfoque en el entretenimiento del consumidor, a pesar de que la misma Nokia venia teniendo éxito con los primeros teléfonos inteligentes basados en el sistema operativo Symbian, y que en Japón ya eran más frecuentes desde 1999. Al mismo tiempo, se estaban popularizando los teléfonos BlackBerry, teléfonos de la empresa Research In Motion que tenían la capacidad de navegar por Internet y revisar el correo electrónico.

Un año después, el 9 de enero de 2007, Steve Jobs anuncia el primer iPhone, que finalmente fue lanzado el 29 de junio y revolucionó el mercado, sumado al lanzamiento un año después del primer móvil con el sistema operativo Android, el T-Mobile G1, que a pesar de que no sería tan exitoso, sentaría las bases de ingreso de Google al mercado de los smartphones o teléfonos inteligentes.

Es así, con las ventas de las computadoras (portátiles y de escritorio), más el auge de los smartphones mencionados anteriormente, Cisco IBSG estima como fecha de nacimiento del IoT algún punto entre el año 2008 y 2009, en esa misma línea, el número de dispositivos conectados a Internet en 2010 ya era de 12,5 mil millones, sobrepasando en tamaño a la población mundial de ese entonces, la cual era de 6.8 millones.(Evans, 2011). Este número ha seguido en aumento, según el estudio de IoT Analytics que menciona que a finales de 2022 ya existen más de 14.400 millones de dispositivos de IoT conectados, teniendo una desaceleración durante la pandemia en 2020, pero repuntando el crecimiento de la cantidad de dispositivos durante este último año, calculando que de 2022 a 2025 el crecimiento se acelere aún más llegando a la cifra de 27.000 millones de dispositivos conectados al IoT en el mundo (IoT Analytics, 2022)

2.3. las ciudades inteligentes y proyección de estas

Durante la siguiente década, se comenzó a analizar por parte de las empresas, la posibilidad de incorporar la tecnología en otros ámbitos que no sea la computación, es así como en 2015 el McKinsey Global Institute intenta determinar cuánto exactamente va a impactar económicamente el IoT en el año 2025, concluyendo que "se estima que el Internet de las cosas tiene el potencial de impacto económico desde 3.8 billones hasta 11.1 billones de dólares al 2025, lo que es equivalente alrededor del 11% de la economía mundial"(Manyika et al., 2015: p. 2). Este estudio refleja claramente lo que ha ido sucediendo desde 2015 hasta la actualidad, en que se ha visto a las empresas de todo ámbito apostar con la tecnología del IoT. En este punto deja de ser algo solo doméstico o limitado a los smartphones y los computadores de escritorio, sino que ahora también el Internet ha llegado a otro tipo de objetos, como los relojes, lentes de realidad aumentada, refrigeradores, inclusive se han llegado a conectar animales, ya sea con chips para saber su localización o para seguir su alimentación. (Barrio, 2020: p. 25)

Finalmente, es importante mencionar a la ciudad inteligente, la cual es definida como como "una ciudad que utiliza las Tecnologías de la Información y Comunicación (TIC), dirigidas a mejorar la calidad de vida de los ciudadanos, y que de manera obligada tendría que preservar el cuidado del medio ambiente y la reducción de la desigualdad social"(Rivas et al., 2022: p. 22). Esta definición la podemos llevar a diferentes ámbitos de uso, en cosas simples como mejorar los tiempos de búsqueda de estacionamiento de automóviles, a temas más complejos como el organizar mejor el tráfico, mejoras en la seguridad, en la salud, etc. Dentro de las principales ciudades inteligentes del mundo podemos encontrar a Shanghái, Seúl, Barcelona, Pekín y Nueva York, esto según el estudio de Juniper Research de 2022, basado la cobertura y la infraestructura del transporte público, la energía que gastan las ciudades, la tecnología que poseen y la conectividad (Moar, Bainbridge, 2022). Este estudio también menciona los gastos que las ciudades inteligentes van a generar en 2026, ascendiendo estos a casi 70 mil millones de dólares, comparados con los 35 mil millones de dólares que se gastaron en 2021 en la tecnología para estas ciudades, por lo que en casi 5 años el gasto se va a duplicar.

3. Regulación actual del Internet de las cosas en Chile

No es de extrañar que en los últimos años los países se vean tentados a impulsar su desarrollo tecnológico cada vez más presente en nuestra sociedad como una manera de modernización y agilización de diversas plataformas que contribuyan a la solución eficaz de las demandas ciudadanas. Es así como en nuestro país se han implementado, aunque de manera insuficiente, diversas regulaciones relacionadas a las nuevas tecnologías tales como la ley 19.223 de delitos informáticos de 1994; la ley 19.628, de protección de la vida privada en 1999, y la ley 19.799, de firma y documentos electrónicos, de 2002.

Es evidente que la regulación mencionada reviste de una significativa desactualización, lo cual es bastante preocupante tomando en consideración no solo el constante avance de las nuevas tecnologías, sino la vulneración de derechos que puede acarrear al no tener un marco normativo eficiente que los proteja e informe, pugnando con estándares, principios y directrices internacionales de la Organización para la Cooperación y el Desarrollo Económico (OCDE) que desde el 2010 Chile se ha comprometido a introducir en su legislación.

Con respecto a las últimas propuestas normativas que se han hecho en torno a los derechos digitales, la Agenda digital 2020 del año 2015 impulsada por Michelle Bachelet, tuvo la intención de encaminar al país hacia la implementación de las nuevas tecnologías a fin de lograr una mayor interconectividad de los ciudadanos en diferentes ámbitos y una creciente modernización de la administración del Estado en un plazo de 5 años. Dentro de ese marco, el año 2017 se presentó al Senado un proyecto de ley consistente en modificar significativamente la ley 19.628 sobre protección de datos personales con el principal objeto de "regular el tratamiento de los datos personales, asegurando el respeto y protección de los derechos y libertades fundamentales de los titulares de datos (personas naturales), en particular el derecho a la vida privada" (Boletín N° 11.114-07, 2017). Este intento de reforma y actualización permanece dormido hoy en día en el segundo trámite constitucional, lo que refleja el poco interés por parte de los gobiernos en promulgar e implementar un pronto marco normativo a este problema que se hace cada vez más presente tanto en nuestro país como en el ámbito internacional.

Finalmente, el último intento por generar un marco normativo en el ámbito del Internet de las cosas y garantizar los derechos fundamentales de los usuarios, en específico el derecho a

la privacidad, es el proyecto de nueva Constitución Política, que fue rechazado sin embargo por la ciudadanía, el cual integraba una serie de artículos sobre derechos digitales, siendo los más relevantes para nuestro tema los artículos 70, 87 y 88.

El artículo 70 de la propuesta consagra el derecho a la privacidad e incluye en su numeral 3 una mención a los metadatos: "Toda documentación y comunicación privada es inviolable, incluyendo sus metadatos. La interceptación, la captura, la apertura, el registro o la revisión solo se podrá realizar con orden judicial previa" (Proyecto Nueva Constitución, 2022). Esto se corresponde con los principios básicos de aplicación nacional de la OCDE, en específico el principio de limitación de recogida que menciona que "deberán existir límites para la recogida de datos personales y cualquiera de estos datos deberán obtenerse con medios legales y justos y, siempre que sea apropiado, con el conocimiento o consentimiento del sujeto implicado.(OCDE, 2002)

El artículo 87 por su parte menciona la protección de datos personales y reconoce los derechos llamados ARCO que otorgan a las personas un mayor manejo de sus datos personales añadiendo el derecho de portabilidad: "Toda persona tiene derecho a la autodeterminación informativa y a la protección de datos personales. Este derecho comprende la facultad de conocer, decidir y controlar el uso de los datos que le conciernen, acceder, ser informada y oponerse al tratamiento de ellos, y a obtener su rectificación, cancelación y portabilidad, sin perjuicio de otros derechos que establezca la ley.

2. El tratamiento de datos personales solo podrá efectuarse en los casos que establezca la ley, sujetándose a los principios de licitud, lealtad, calidad, transparencia, seguridad, limitación de la finalidad y minimización de datos." (Proyecto de Nueva Constitución, 2022)

Esto es un gran avance en relación con el cumplimiento del marco regulatorio internacional y de los principios establecidos por la OCDE.

Finalmente, el artículo 88 refuerza esta idea de la privacidad y protección de los datos personales con relación a la seguridad informática: "Toda persona tiene derecho a la protección y promoción de la seguridad informática. El Estado y los particulares deberán adoptar las medidas idóneas y necesarias que garanticen la integridad, confidencialidad, disponibilidad y resiliencia de la información que contengan los sistemas informáticos que administren, salvo los casos expresamente señalados por la ley." (Proyecto Nueva Constitución, 2022)

4. Problemática actual en relación con el derecho a la privacidad

El acelerado crecimiento de las nuevas tecnologías y la necesidad de volver estas más eficientes en cuanto a su funcionamiento ha dado paso a que la información personal de los usuarios recopilada para este fin se encuentre en un delgado hilo que lo separa de la transgresión del derecho a la privacidad.

En este sentido, el consentimiento de las personas juega un rol fundamental a la hora de solicitar y de utilizar estos datos recopilados, no solo en su forma expresa al momento mismo de autorizar dichas prácticas sino también en la correcta e íntegra información proporcionada al titular de los datos personales sobre ese uso con la debida antelación dado que en la mayoría de los casos los usuarios suelen dar su consentimiento a las empresas sin saber realmente lo que están permitiendo. Como señala la Comisión de la Unión Europea (2015), "que los consumidores no sepan qué datos suyos son recolectados y cómo son usados, constituye una asimetría de información entre los actores del mercado, lo que puede interferir con sus derechos fundamentales a la privacidad y a la protección de datos personales y puede resultar en una violación al derecho a no ser discriminado." (Jervis, 2016: p. 29)

Es por lo anterior que el principal problema en la transgresión del derecho a la privacidad de los consumidores producto del Internet de las cosas dice relación con la forma en que las empresas utilizan estos datos, siendo más específicos, cuando las empresas no les dan el fin para el cual fueron almacenados, como por ejemplo la creación de perfiles sobre las personas para la venta de seguros.

Asimismo, se transgrede el derecho a la privacidad cuando la información recopilada excede de aquella requerida para el objetivo que se consintió en primer lugar o cuando esta misma información sobrepasa una cantidad ética en su acumulación, por lo que "no hay que ir demasiado lejos para entender la preocupación: en la propia visión de una red omnipresente de objetos y dispositivos subyace un sistema robusto de vigilancia del individuo"(Cortez, 2014: p. 11), mientras más dispositivos inteligentes conectados existan en nuestra sociedad, mayor será la cantidad de datos que recopilen de nuestra vida diaria y aun cuando consintamos en ello, esta

forma silenciosa de operar hace que no nos demos cuenta de la magnitud de información entregada y por consiguiente nuestra privacidad se ve sobreexpuesta a una serie de problemas que conlleva esta omnipresencia del Internet de las cosas como pueden ser la intercepción o monitoreo de estos datos para usos maliciosos si es que el usuario es una persona de interés público.

Otro de los problemas a considerar tiene relación con el nivel de control de los datos personales propios que permiten las empresas e instituciones manejar una vez ya recopilados, la prohibición del manejo de nuestra información no debe ser nunca producto de la entrega consentida de estos en ningún caso, es por esto que "el derecho a la protección de datos personales busque tutelar a las personas, mediante el otorgamiento de un poder de control sobre su propia información, sujeto a ciertas restricciones susceptibles de ser valoradas bajo márgenes de apreciación que comprendan tanto los requisitos que permiten justificar una injerencia como la gravedad de la afectación respecto de otros derechos humanos" (Solange et al., 2017: p. 94)

Este tema del poder que tenemos sobre nuestra información personal y la necesidad de borrar nuestros datos o de prohibir que se sigan utilizando una vez cumplido el propósito para el cual se recopilaron se manifiesta en los llamados derechos de supresión, bloqueo y oposición reconocidos por el Reglamento Europeo de Protección de Datos Personales, este menciona que "el derecho al olvido que nace de la relación de los derechos de supresión, bloqueo y oposición, ya reconocidos en las legislaciones protectoras de datos, busca que los sujetos tengan la facultad de exigir que sus datos personales sean completamente eliminados de cualquier tipo de registro, de manera tal que ya no se pueda efectuar una vinculación a ninguno de ellos." (Jervis, 2016: p. 37)

Podemos concluir entonces que el factor de mayor importancia a la hora de encontrarnos frente a vulneraciones al derecho de privacidad entorno al Internet de las cosas es el consentimiento, la falta de consentimiento informado eficazmente acarrea una serie de problemas que como ya hemos visto dificultan una buena integración del Internet de las cosas a nuestra vida diaria.

5. Proyección a futuro

A medida que la tecnología avanza los dispositivos van mejorando en su capacidad de recolectar información logrando ser cada vez más imperceptibles a la hora de extraer y almacenar

nuestros datos personales, este fenómeno amplía las probabilidades de vulnerar los derechos fundamentales de los ciudadanos, y en especial el derecho de privacidad, sobre todo si no se aplica un debido marco legal que regule todos los ámbitos en los cuales se ven comprometidos los principios guías del Internet de las cosas y la protección de datos personales.

Es por esto que lo que se espera con un nuevo y actualizado marco regulatorio y normativo es por un lado fomentar y avanzar en nuestro país hacia lo que son las ciudades inteligentes, en las cuales se busca sacar el mejor provecho a la tecnología en favor de las personas y de sus intereses y necesidades facilitándoles la vida cotidiana mediante objetos sin transgredir los derechos de los ciudadanos y por otro lado limitar el desenfrenado y silencioso uso y manipulación de los datos personales por parte de las empresas y servicios para fines que no le fueron concedidos.

En caso contrario, de seguir dormido el Proyecto de Ley del boletín N° 11.114-07 en el Congreso, la desactualización del marco normativo e institucional provocará más que un estancamiento en materia de derechos digitales, un retroceso, impidiendo que las personas naturales acepten la implementación de estas tecnologías en su vida diaria producto de la desconfianza que produce esta falta de regulación tanto en la administración del Estado como en las empresas, es por esto que "la protección efectiva de la información personal, mediante el derecho sustantivo, la existencia de autoridades de control independientes, las normas procedimentales y sancionatorias, así como los mecanismos de cooperación adecuados, son la base para generar esta confianza, necesaria en todos los ámbitos, sea en las relaciones entre particulares y las Administraciones Públicas como respecto de los consumidores y proveedores de bienes y servicios que tratan datos personales." (Solange et al., 2017: p. 94)

Además, como bien se ha mencionado, Chile ya se encuentra en la mira de los organismos internacionales puesto que hasta la fecha no se ha dado cumplimento a lo comprometido en favor de la promoción de los derechos y principios digitales y de su respectiva limitación, pudiendo ser en un futuro causa de algún tipo de sanción por incumplimiento de los compromisos internacionales que suscribió.

Dado lo anterior, parece de suma importancia tomar medidas lo más pronto posible mientras la realidad de nuestro país en torno al Internet de las cosas aún no logra superar el umbral de las ciudades inteligentes por lo que la recopilación de datos personales no está en un nivel

preocupante, esto con intención de que no nos tome desprevenidos y sin las herramientas necesarias para afrontarla en un futuro cercano dado que "la captura masiva de información personal en tiempos del IoT es distinta –y más preocupante– que la actual por varias razones: primero, se capturará información en muchos lugares más; segundo, el acopio será invisible; tercero, los datos serán más íntimos, y cuarto, las facilidades de interconexión conllevarán a que nuestros datos sean compartidos en niveles nunca antes vistos."(Cortez, 2014: p. 12)

Capítulo II: Análisis de la Regulación en Chile y su aplicación

1. Análisis de la ley 19.628

1.1. Críticas a la ley

El contexto histórico en el que se enmarca el nacimiento de la ley 19.628 data del año 1999, si bien su dictación constituyó un gran avance en una sociedad que no contaba con un acceso masivo al Internet, hoy en día con el desarrollo de la tecnología digital y la expansión del comercio electrónico se ha producido un acelerado intercambio de información haciendo que esta ley no cubra todos los aspectos en que este flujo y manejo de datos afecta la privacidad de las personas resultando insuficiente para el fin originalmente perseguido.

Esta ley si bien contiene una serie de principios y garantías protegiendo a los usuarios frente al tratamiento de datos personales, otorgándoles derechos como el de acceso, de modificación, de bloqueo y de cancelación de datos a través de un requerimiento a quien sea responsable de un banco y de manera gratuita según lo dispone el artículo 12, deja al debe una serie de ámbitos fundamentales para la debida protección del derecho a la privacidad tanto de personas naturales como jurídicas.

En primer lugar, existe un grave problema relacionado a la poca fiscalización y control de la actividad de tratamiento de datos personales en que en muchas ocasiones la falta de información por parte de aquellos organismos encargados de la recopilación de datos produce que las personas naturales no tomen conocimiento de haber firmado contratos formulados en base a prestar su consentimiento dada la magnitud del desarrollo de las nuevas tecnologías en que el trato mayormente es impersonal, reduciéndose a la aceptación de términos y condiciones

con un solo clic, entonces si bien la ley tiene una fuerte tendencia a que los usuarios puedan autodeterminar el uso que se haga de sus antecedentes cuando son registrados y almacenados, este propósito no es eficaz toda vez que no contempla un mecanismo de control sobre la forma en que se obtienen.

Dado lo anterior, esta falta de control e información producen en diversas ocasiones que los consumidores ni siquiera se enteren de que efectivamente su derecho a la privacidad está siendo vulnerado permitiendo que aquellos organismos dedicados al almacenamiento y tratamiento de datos personales pasen desapercibidos debido a la falta de certeza en el flujo de información, con lo cual se produce una situación en que la ley opera de tal manera que se enfoca mayormente en que los consumidores vean primero su derecho fundamental vulnerado para ejercer su protección en vez de tender a evitar que estas vulneraciones sucedan.

La ley tampoco contempla un límite en cuanto al organismo o entidad encargada de almacenar y tratar estos datos por lo que podemos inferir que cualquier persona, sea natural o jurídica, pública o privada puede constituir un registro o banco de datos sin ningún tipo de control dado que ya que "es importante resaltar que la ley no contempla organismos administrativos a cargo del control de esta actividad y el principio, en definitiva, es que cualquier persona puede efectuar el tratamiento organizado de datos en la forma que dispone la ley, sin necesidad de registro previo." (Vial, 2001: p. 34) Esto a excepción del artículo 22 que obliga a los organismos públicos a informar y registrar en el Registro Civil e Identificación la creación de bancos de datos personales indicando el fundamento jurídico, tipos de datos almacenados y descripción del universo de personas que comprende lo cual que no aplica para entidades particulares constituyendo una omisión grave por parte de la ley a este respecto.

Lo anterior resulta preocupante dado que precisamente son los organismos estatales quienes tienen un mejor fundamento o justificación para almacenar datos personales fundados en razones de orden público, no así, las empresas e instituciones privadas quienes en general al tener un fundamento puramente económico o comercial son más propensas a incluir cláusulas abusivas en los contratos de prestación de consentimiento y a difundir o compartir información personal de sus usuarios que no les corresponde dando como resultado abusos que transgreden la vida privada de las personas.

Otra de las falencias que presenta esta ley es que no contempla entre sus definiciones ni principios el llamado "derecho al olvido" el cual se ha adoptado a nivel internacional frente a la necesidad de que las personas vean su esfera privada protegida al momento de ser buscados en Internet ya que debido a su masificación es actualmente la fuente principal de acceso a la información. Lo anterior impide que se ejerza en su totalidad el derecho de cancelación de datos que supone la destrucción de los datos almacenados en registros o bancos de datos dado que no contempla los llamados motores de búsqueda dentro de la definición legal de registro o banco de datos, quedando expuesta la información personal de las personas sin que consientan en ello, aun cuando se haya solicitado su eliminación de la base de datos que originalmente los recopiló, es así como "en la práctica, el derecho al olvido en Internet no es otra cosa que una definición de política pública que declara a los motores de búsqueda como responsables de bases de datos, lo que permite que los titulares de datos personales puedan hacer efectivo su derecho a cancelación de estos datos respecto del buscador." (Mesías y Viollier, 2021: p. 80)

Otro punto para considerar es que la ley, dentro del ámbito de los datos personales, hace una distinción entre los datos sensibles y los datos puramente personales, siendo estos últimos su objeto de regulación y dependiendo de su fuente de obtención estos pueden ser de acceso público o privado. Aquí nos encontramos con un problema puesto que si bien el consentimiento del titular de los datos es esencial para el tratamiento de estos el artículo 4 inciso quinto excluye este principio para algunos casos de datos personales de acceso público de los cuales tampoco requieren de una finalidad particular para su tratamiento y que si bien esta excepción es taxativa la ley es bastante amplia en cuanto a lo que considera como base de datos de fuente accesible al público recayendo en el titular de ellos la facultad de dejar abierto al público el registro. Lo anterior es especialmente preocupante dada la actual masificación de las redes sociales y el acceso a Internet en la que podrían al tenor de la ley ser consideradas como fuente de acceso público y haciendo excepción al principio general del consentimiento lo cual da cabida a una mayor vulnerabilidad de la privacidad de las personas.

Finalmente, esta ley en cuanto a su redacción y a lo establecido en su artículo 2 letras f) y ñ) excluye de su ámbito de aplicación a las personas jurídicas contemplando un margen regulatorio exclusivamente para las personas naturales. Consideramos que la confidencialidad y reserva de la información sobre las personas jurídicas es igualmente relevante como lo son de

las personas naturales, al ser sujeto de derechos, y en su calidad de personas, merecen el resguardo y la protección de sus datos frente a posibles abusos de sus antecedentes propios o en el erróneo procesamiento de estos.

1.2. Aplicación de la ley en Chile

Él ámbito de aplicación esta ley tiene por objeto regular el tratamiento de datos carácter personal, por personas naturales u organismos públicos o privados que se efectúen en registros o bancos de datos y que no se encuentre regido por una ley especial.

La ley en este sentido en cuanto al tratamiento de datos este se refiere a "cualquier operación o complejo de operaciones o procedimientos técnicos, de carácter automatizado o no, que permitan recolectar, almacenar, grabar, organizar, elaborar, seleccionar, extraer, confrontar, interconectar, disociar, comunicar, ceder, transferir, transmitir o cancelar datos de carácter personal, o utilizarlos en cualquier otra forma"(Ley 19.628, 1999), según su artículo 2 letra o, el cual también abarca una gran cantidad de acciones relacionadas a los datos personales incluso dejando abierto a cualquier forma de utilización que no se encuentre regulada en la ley.

Como ya mencionamos anteriormente, esta ley protege únicamente de manera expresa los datos de las personas naturales ya que, si bien en muy pocos casos la Corte Suprema con el fin de resguardar el derecho a la vida privada de las personas ha debido interpretar esta ley de manera extensiva, aún existe controversia en aceptar la legitimación activa de las personas jurídicas por lo que su aplicación ha sido escasa.

Como podemos observar la ley está dirigida principalmente a regular el tratamiento de datos realizado por registros o bancos de datos que manejan información a mayor escala y no así entre particulares, como es el caso de las redes sociales, o aparatos electrónicos que almacenan información personal quedando excluidos de esta regulación

1.3 Procedimiento especial, Habeas Data

En primer lugar, los derechos que establece la ley se deben hacer valer ante la persona natural o jurídica u organismo público que mantenga un registro o banco de datos mediante un requerimiento de manera gratuita. Si la solicitud de acceso, modificación, bloqueo, cancelación, copia u oposición es denegada por el responsable o no se pronuncia sobre esta procede la acción amparo digital o más conocido como Habeas Data interpuesto ante el juzgado civil del lugar de domicilio del responsable de datos, el cual es un procedimiento especial, específico y autónomo creado por esta ley en su artículo 16 inciso primero, específicamente para resolver este tipo de controversias.

Además de este procedimiento especial la ley también contempla la posibilidad de ejercer una acción civil con el fin de indemnizar los perjuicios causados y la constatación de responsabilidad infraccional según se aprecia de los artículos 23 y 16 inciso final. Al no existir una entidad reguladora autónoma de esta materia para regular las controversias dadas por la no aplicación de la ley los usuarios deben recurrir a los tribunales de justicia soportando el costo y el largo tiempo de espera que esto significa.

Aun cuando existe este procedimiento especial la realidad es que en la práctica la acción ejercida para este tipo de vulneraciones es el recurso de protección y aunque se ha alegado en varias ocasiones que no es el procedimiento correcto dada la existencia de una acción especial legalmente establecida, la Corte Suprema ha dicho que "cabe señalar que la existencia de un procedimiento especial contemplado en la Ley N° 19.628 no obsta al ejercicio de la acción de protección, porque ésta puede ejercerse sin perjuicio de otros derechos" (SCS 11.256/2011, de 27 de enero, C. 6°). Esto dado la posibilidad de ejercer el habeas data posteriormente como también sucede con el amparo económico.

Lo anterior demuestra una clara ineficacia por parte de la ley al momento de hacer valer nuestros derechos sobre todo en lo que respecta al derecho a la vida privada dado que "el procedimiento específicamente creado para las controversias que se susciten sobre los supuestos planteados por esta ley ha resultado prácticamente inutilizado ante las tentaciones del recurso de protección, acción que se ha mostrado como una efectiva herramienta ante la publicación de información comercial carente de sustento legal"(Rostión, 2015: p. 500). Por tanto, podemos

deducir que a pesar de las intenciones de esta ley de crear un procedimiento específico para esta materia e intentar incorporar el Habeas Data a nuestra legislación estas fueron insuficientes en la práctica produciendo un desconocimiento de esta vía volviéndola casi innecesaria frente a mejores opciones, esto probablemente por consagrarse en una ley y no en la constitución como si lo han hecho otros países dada la importancia de este procedimiento.

2. Análisis al proyecto de ley que la modifica

El proyecto de ley que modifica la ley 19.628 data del 15 de marzo de 2017 y actualmente continúa en discusión en la Cámara de Diputados. Si bien el proyecto cuenta con "urgencia suma" legislativa aún falta para que podamos ver surgir este nuevo y actualizado marco regulatorio y más aún su implementación y eficacia a la hora de proteger nuestros derechos y en especial nuestra vida privada. En este apartado nos enfocamos en analizar lo que a nuestro parecer son algunas de las modificaciones a la ley más relevantes en torno a la efectiva protección de la vida privada en relación con los datos personales.

Este proyecto busca de manera general modernizar el marco normativo de la protección de datos personales permitiendo enfrentar los desafíos digitales del siglo XXI y concordar con la normativa internacional y los compromisos adquiridos por Chile con su entrada a la OCDE. También pretende hacerse cargo de la evidente colisión de derechos tratando de equilibrar derechos fundamentales de las personas tales como el respeto y protección a la vida privada e intimidad, con el derecho a la libre circulación de la información.

Uno de los ejes principales a considerar del proyecto es que pretende poder consagrar en nuestra legislación el ya mencionado "derecho al olvido" agregando dentro de sus definiciones legales del artículo 2 la de "motor de búsqueda" estableciendo además que "En relación con los resultados de búsqueda, el titular de datos personales podrá ejercer el derecho de cancelación contemplado en la presente ley, sin perjuicio de los demás derechos que establece esta ley, cuando correspondan" (Boletín 11.144-07, 2017). Esto supone un gran avance dado que extiende la regulación del tratamiento y protección de los datos personales hasta el Internet, incorporándolo dentro de la esfera de su aplicación e incluyéndolo en el derecho de cancelación (el cuál es irrenunciable) permitiendo que, a pesar de estar limitado por el derecho a la

información, libertad de prensa y de investigación, aquella información recabada legítimamente se retire una vez agotada su finalidad para la que fue obtenida, resguardando así de manera más eficaz la privacidad de las personas y fomentando la autodeterminación informativa.

Con relación al consentimiento también vemos una gran mejora puesto que también se agrega como definición en el artículo 2. Pasamos de un sistema de autorización escrito a uno en que el consentimiento es tratado como regla general y puede ser expresado de manera verbal, escrita o a través de un medio electrónico equivalente o mediante un acto afirmativo. El consentimiento incluye a toda manifestación de voluntad que debe ser libre, específica, inequívoca e informada y que además abre la posibilidad de consentir bajo representación. Para el caso de contratos o prestaciones de servicio que no necesitan el tratamiento de datos personales para su ejecución o cumplimento se presume que el consentimiento otorgado no ha sido libre, además corresponde al responsable de datos probar que el tratamiento fue realizado con el consentimiento del titular. Lo anterior da cuenta del intento por parte de este proyecto de equilibrar la posición entre el titular de los datos personales y el responsable dado que la cantidad de información que maneja cada uno acerca del producto o servicio que se está prestando es proporcionalmente desventajosa para los usuarios.

También, buscando dar cumplimiento a los compromisos internacionales asumidos por Chile y en especial con la OCDE se reconocen los derechos ARCOPI en su artículo 5 y siguientes. Estos derechos comprenden el derecho de acceso, derecho de rectificación, derecho de cancelación, derecho de oposición, el derecho de portabilidad y el derecho a la impugnación frente a decisiones automatizadas. Al ser derechos personalísimos estos pueden ser ejercidos solamente por el titular de los datos o su representante por lo que son intransferibles e irrenunciables, pero sí transmisibles a sus herederos, además los derechos de rectificación, cancelación, oposición e información son gratuitos en cuanto a su ejercicio. Una mención expresa a estos derechos supone una mejora en la regulación a la protección de los datos personales toda vez que proporciona un mayor manejo y control para los usuarios de su propia información personal otorgándoles herramientas específicas de reclamación ante posibles vulneraciones, además se especifica en qué consiste cada uno de estos derechos por lo que las personas pueden identificar más fácilmente las medidas a las cuales puede optar toda vez que pueda ver afectado su derecho a la privacidad.

Finalmente este proyecto plantea la creación de una autoridad de control en torno al tratamiento de datos, esta es, la "Agencia de Protección de Datos Personales" el cual es un organismo público, autónomo y de carácter técnico con la capacidad de fiscalizar, regular y sancionar los incumplimientos de la ley mediante la aplicación de multas de hasta 10.000 UTM para infracciones gravísimas en materia de protección de las personas y tratamiento de datos personales lo cual es muchísimo más alto en comparación a la multa máxima anterior de 50 UTM atendiendo que estamos hablando de incentivos para que grandes administradoras de datos cumplan la ley . La creación de esta agencia es a nuestro parecer el agregado más importante que hace este proyecto en cuanto a la aplicación de la ley 19.628 puesto que es un gran avance en la eficacia de la protección de los derechos de los titulares de estos datos lo cual requiere de una entidad que haga cumplir la legislación y fiscalice su cumplimento garantizando la protección a la vida privada de las personas. Además, en el proyecto se crea el llamado "Registro Nacional de Cumplimiento y Sanciones" el cual es de carácter público y administrado por la Agencia, este se encarga de consignar los modelos certificados de prevención; los responsables de datos que los hayan adoptado; las sanciones que se hayan impuesto a los responsables de datos que hayan infringido la ley, y aquellos a quienes se les haya revocado la certificación (Boletín 11144-07, 2017, aquí podemos observar la intención de este proyecto de no solo sancionar a aquellos infractores de la ley sino también prevenir que se cometan vulneraciones a sus usuarios mediante este sistema de certificación para aquellos bancos o registros de datos que se apeguen a la normativa, además permite a las personas obtener información de aquellos organismos que hayan sido sancionados anteriormente o que se les haya revocado su certificación consagrando un mayor nivel de transparencia en este ámbito y protegiendo de mejor manera el derecho a la privacidad.

3. Análisis de jurisprudencia

Para un mejor acercamiento de cómo funciona la protección de este derecho en la práctica y su aplicación por los Tribunales de Justicia es necesario analizar la jurisprudencia correspondiente de la cual se señalan diferentes puntos a considerar entorno al derecho a la privacidad.

El primer caso es el de un ex carabinero procesado y condenado por una situación de abuso sexual quien tras cumplir condena por el delito que cometió, seguía siendo asociado con su nombre a la causa en los buscadores de Internet, provocándole un perjuicio al momento de rehacer su vida en busca de reinserción social. Aquí primeramente se recurrió contra el Diario el Mercurio para que procediera la eliminación de la publicación de Internet en EMOL.COM y al no obtener respuesta se presentó un recurso de protección ante la Corte de Apelaciones sentencia que fue revocada por la Corte Suprema en causa Rol N° 22.243-2015, de 21 de enero de 2016, ordenando la eliminación de la noticia basándose en el derecho al olvido.

Cabe destacar que la vulneración en el derecho a la privacidad alegado en este caso no solo se presenta en la figura del demandado sino hacia toda su familia puesto que el apellido de este no es común.

Nos pareció interesante analizar esta sentencia puesto que se observa un reconocimiento en la jurisprudencia chilena a lo que es el llamado derecho al olvido el cual como hemos mencionado, y como bien se menciona en la sentencia, no se encuentra consagrado en nuestra legislación. La Corte Suprema utilizó como base de su fundamentación tratados y criterios internacionales para resolver que en base al factor tiempo la noticia en cuestión dejó de cumplir su finalidad por lo que se debe priorizar el derecho al olvido por sobre el derecho a la información con el fin de garantizar a las personas la satisfacción del derecho a la privacidad tal como demuestra su considerando cuarto al mencionar que "no cabe duda que nuestro ordenamiento jurídico protege el honor y vida privada de las personas en cuanto tales, incluso antes y después de su constitución jurídica; y que sistemáticamente ha venido recogiendo la tendencia mundial de reconocer el derecho al olvido respecto de conductas reprochables de las personas –sean éstas penales, civiles o comerciales- después de un lapso de un tiempo, como una forma de reintegrarlas al quehacer social."(SCS 22.243/2015, 21 de enero, C. cuarto)

El segundo caso trata de una sentencia pronunciada por el 16° Juzgado Civil de Santiago causa Rol C-29221-2015 la cual condenó a un banco de datos a indemnizar por daño moral a tres de sus clientes. Se determinó que el demandado infringió los artículos 6 y 11 de la Ley N° 19.628 y se le condenó a pagar dos millones a cada uno por concepto de daño moral. En este caso se encontraron documentos abandonados en un basural clandestino que contenían información personal de los clientes del demandado incluyendo cédulas de identidad, situación

financiera, evaluaciones crediticias, liquidaciones de sueldo, cheques, información de dineros en cuentas personales, etc.

En este caso el derecho a la vida privada fue fuertemente violentado puesto que la información personal de los clientes fue expuesta de manera tal que cualquier persona que se percatara de los documentos podía invadir la privacidad de las personas afectadas, lo cual representó un sufrimiento por el actuar negligente del responsable de datos además de traicionar la confianza en el mismo mereciendo una compensación económica por este pesar.

Esta es una sentencia interesante puesto que si bien la ley dispone en su artículo 23 que el tratamiento indebido de los datos es susceptible de indemnización por daño moral , no es usual que los tribunales acepten esta indemnización del daño físico o psicológico en materia de protección de datos, esto da cuenta de la importancia que ha ido tomando con los años en la judicatura la necesidad de una reparación completa al momento de transgredirse estos derechos consagrados en la ley y la relevancia de los datos personales en nuestra sociedad.

Finalmente, el tercer caso es una sentencia dictada por la Corte Suprema causa Rol Nº 7148-2015, que revoca la sentencia apelada acogiendo el recurso de protección. El recurso fue deducido por una publicación en la red social Facebook de una noticia relacionada con una prestación de servicio que no se llevó a cabo por el demandante en la cual se adjuntó la fotografía correspondiente a la contenida en la cédula de identidad del actor la cual fue obtenida sin su consentimiento recibiendo burlas e insultos hacia su persona.

El demandante en este caso había otorgado una copia de su cédula de identidad al momento de suscribir el contrato de prestación de servicio frente a un notario con la finalidad de comprobar su identidad, sin embargo, no prestó su consentimiento para que la foto fuera utilizada para la publicación de la noticia. Llama la atención esta sentencia puesto que a pesar de que la Corte Suprema ordenó la eliminación de la fotografía de la cédula de identidad del actor por determinarse que correspondía a un uso no autorizado de la imagen propia el cual según la doctrina y jurisprudencia se encuentra comprendido en el derecho de privacidad, se da importancia a que la fotografía en cuestión no se encontraba disponible en su cuenta de Facebook ni en ningún otro sitio web de acceso público enfatizando en las políticas de la plataforma de Facebook en su considerando décimo en el cual se menciona: "Que, por otra parte, Facebook bajo el capítulo "Condiciones" en el acápite relativo a "privacidad", establece:

"4. Cuando publicas contenido o información con la configuración "Público", significa que permites que todos, incluidas las personas que son ajenas a Facebook, accedan a dicha información, la utilicen y la asocien a ti (es decir, a tu nombre y foto del perfil)". (SCS 7.148/ 2015, de 14 de septiembre, C. 10°)

Lo anterior nos permite deducir que si la foto mencionada o en general cualquier otra información personal se encuentra de manera pública ya sea en Facebook o en cualquier otra red social o plataforma digital de libre acceso es posible hacer uso de aquellos datos o imágenes sin requerir un consentimiento previo dejando la responsabilidad de protección de la privacidad a los propios titulares de datos. Dada la masificación del fenómeno de las redes sociales este sistema de privacidad para controlar quienes tiene acceso a nuestra información personal nos resulta deficiente dado que no todos los usuarios cuentan con el mismo conocimiento como para entender lo que significa que estas plataformas se reconozcan como fuentes de acceso público puesto que no existe como sociedad una conciencia colectiva respecto a este tema. Además, no todos se manejan con la misma prudencia o precaución en cuanto a las plataformas digitales, esto teniendo en cuenta que en la actualidad tanto adultos mayores como menores de edad hacen uso de estas.

Capítulo III: El Derecho comparado: El lugar al que realmente queremos ir

1. Regulación Europea al Internet de las cosas

El continente europeo es uno de los lugares del mundo en el cual más avance se ha hecho en relación con regulación del derecho a la privacidad dentro del ámbito del Internet de las cosas. En este capítulo se analizará la regulación dentro del Derecho de la misma Unión Europea, para luego entrar al Derecho comparado de algunos de los países con mayor regulación sobre esta materia en el continente como lo son España e Inglaterra.

1.1. Leyes de la Unión Europea

La Unión Europea comienza a regular el Internet de las Cosas desde una cierta base de desconfianza frente a las empresas y los desarrolladores de aparatos electrónicos, por lo que se entiende que, en base a esta desconfianza, el Estado busque proteger a las personas frente a estas nuevas tecnologías, por lo que se dice en Europa que "la regulación se considera fundamental para proteger la equidad y competencia"(Feldgen, 2018). Una manera de proteger esta equidad y competencia que se mencionaba anteriormente es por medio de la Comisión Europea, que es una de las instituciones de la Unión Europea, encargada de regular estos asuntos promoviendo investigaciones, controlando el desarrollo y fijando políticas en todos los países miembros del bloque.

Estas políticas tuvieron un giro dramático en el continente el año 2014 con la sentencia del Caso Costeja[1], cuyo litigio finalmente decanto por una protección más dura al derecho a la privacidad de las personas, en su esfera del derecho al olvido cibernético, el cual lo podemos definir como el derecho "a que la información publicada en línea en Internet no permanezca fija e intangible, ya que todas las personas tienen una segunda oportunidad"(Bobadilla, 2020: p. 123), como también a la protección de los datos personales, ya que Google tuvo que borrar todas las referencias al caso de embargo que afectaba al señor Costeja. Esta sentencia fue dictada por el Tribunal de Justicia de la Unión Europea, el que determinó el borrado de la información, pero además sentó un precedente porque el mismo tribunal sentenció que cualquier ciudadano perteneciente a la UE puede solicitar la eliminación de datos del buscador, siendo una de las primeras regulaciones reales en ese continente para proteger el derecho a la privacidad de las personas.

Este caso impulsó también la actualización de la antigua Directiva 95/46 de la UE, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de esos datos, la cual se mantenía vigente desde el 24 de octubre de 1995 en el continente europeo, todo esto porque con las nuevas tecnologías se consideró que había quedado obsoleta, por lo que fue cambiada en 2018 por el Reglamento (UE) 2016/619 del Parlamento Europeo y del Consejo, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, mejor conocido

[1] El cual era un reputado empresario catalán que había sido protagonista de una noticia en un diario español, en relación con un embargo por deudas a la seguridad social española, por lo que cada vez que ponía su nombre en el buscador aparecía esta noticia que le terminaba dando muy mala fama, por lo que solicitaba que esta noticia ya no fuera accesible cuando su nombre se escribía en el buscador de Internet.

como Reglamento General de Protección de Datos, desde ahora RGDP por sus siglas, el que plantea en el considerando 6 que *"La rápida evolución tecnológica y la globalización han planteado nuevos retos para la protección de los datos personales. La magnitud de la recogida y del intercambio de datos personales ha aumentado de manera significativa. La tecnología permite que tanto las empresas privadas como las autoridades utilicen datos personales en una escala sin precedentes a la hora de realizar sus actividades. Las personas físicas difunden un volumen cada vez mayor de información personal a escala mundial." (Reglamento 2016/619, 4 de mayo)*

Por lo que se da a entender este reglamento viene a proteger el derecho a la privacidad en sus esferas relacionadas a las nuevas tecnologías como el Internet de las cosas, y el derecho a protección de datos personales, como también la esfera de aplicación como el derecho al olvido en el sentido que anteriormente se explicó. Esto lo podemos ver aplicado en el artículo 17 del mismo cuando menciona que "el interesado tendrá derecho a obtener sin dilación indebida del responsable del tratamiento a la supresión de datos cuando concurra alguna de las siguientes circunstancias:

1. Estos datos personales ya no sean necesarios en relación con los fines para los que fueron recogidos o tratados.
2. El interesado retire el consentimiento.
3. Los datos personales hayan sido tratados ilícitamente.
4. Los datos personales deban suprimirse para el cumplimiento legal en el Derecho de la Unión o los Estados miembro.
5. Los datos personales se hayan obtenido en relación con la oferta de servicios de la sociedad de la información.

En cuanto al Internet de las cosas, este mismo reglamento se basa en el principio de que los "datos personales de cada persona son propiedad de cada ciudadano" (Feldgen, 2018). Estos datos para ser almacenados por parte de las empresas necesitan también un consentimiento previo (Articulo 6), este consentimiento tiene las siguientes bases según el artículo 7 del mismo:

1. Demostrar que el consentimiento se dio
2. Se podrá retirar el consentimiento en cualquier momento

3. Se tendrá que evaluar si el consentimiento se dio libremente

Otro asunto importante es que el reglamento asegura la transparencia del trato de la información, esto según el artículo 12 que establece que el responsable de tener la información tendrá que facilitar en cualquier momento su derecho al acceso a la información al interesado

Además, dentro de otros tipos de regulaciones, tenemos la Directiva 2013/40, la cual habla sobre los ciberataques y las infracciones a los sistemas que contienen la información, desde el articulo 9 hasta el 11, se ven las sanciones para aquellos que vulneran los sistemas electrónicos como en casos de hackeos y otros tipos de vulneraciones, esto es importante para asegurar un correcto funcionamiento del IoT y para poder mantener la seguridad dentro de los sistemas o "nubes" que mantienen almacenada toda la información y privacidad de las personas que tienen los productos, de igual manera, este reglamento ayuda a estandarizar el sistema de ciberseguridad de todos los países miembros de la UE

Antes de terminar, es necesario mencionar que el desarrollo investigativo del IoT no solo es para regularlo, sino que también para hacer un análisis de mercado, ya que recientemente fue publicado por la Comisión Europea un reporte para el Consejo y el Parlamento Europeo sobre una investigación sectorial sobre el Internet de las cosas del consumidor[2], reporte que fue comenzado en 2020 y publicado durante 2022, el cual se focaliza solo en el IoT en cuanto al sector comercial y en que plataformas se enfoca más la venta de dispositivos, como apartados importantes se confirma el crecimiento del IoT en el mundo, aumentando de 105,7 billones de euros a aproximadamente 404,6 billones de euros al año 2030 (tal como se mencionó en el primer capítulo), además se puede observar que las principales plataformas que ocupan las personas fuera de los televisores y teléfonos inteligentes en Europa son las asistentes de voz, siendo las principales Alexa de Amazon, la asistente de Google y Siri de Apple (European Commission, 2022). Sin embargo, en este mismo reporte se señalan grandes preocupaciones en diferentes ámbitos, una de ellas es la imposibilidad de utilizar en un mismo dispositivo, ya sea celular o computadora, diferentes asistentes de voz al mismo tiempo, lo que podría generar prácticas monopólicas de las empresas ya que estarían obligando al consumidor de ciertas marcas

[2] Report from the commission to the council and the European parliament: Final report – Sector inquiry into consumer Internet of Things en su idioma original

a usar el asistente de voz de su misma línea. Pero lo más importante surge en el tema de la información, pues como se expresó antes una gran preocupación frente a la cantidad de información que pueden almacenar las grandes empresas que poseen asistentes de voz, porque estos asistentes las estarían posicionando en un lugar privilegiado en el mercado, aprovechándose de la información que estos captan para poder publicitar otros dispositivos de su marca.

Finalmente, hay que mencionar que la Unión Europea a pesar de tener una de las regulaciones más avanzadas frente a las amenazas que puede contener el IoT al derecho de la privacidad, en todas sus esferas, aún hay un largo camino por delante para lograr una mejor regulación del acceso a la información privilegiada que las empresas pueden llegar a utilizar para posicionarse dentro de los mercados. Es por esto que la Comisión Europea para el periodo de 2021 a 2027, está invirtiendo aproximadamente €95.5 Millones de euros en investigación, innovación y desarrollo de las tecnologías emergentes relacionadas al IoT, todo esto bajo la creación del programa *Horizon Europe*[3], dentro de este programa también se tiene en consideración de que el IoT debe ser la clave para concretar la transformación digital en aquellos sectores importantes de la sociedad en que la digitalización aún no se da del todo como lo son la industria de la agricultura[4], la energía y la movilidad (European Commission, 2020). De aquello se encarga la Dirección General de Sociedad de la Información y Medios de Comunicación (Desde ahora DG Connect por sus siglas en ingles)[5], uniendo fuerzas con otras direcciones generales para cubrir todos los puntos posibles, promoviendo así programas en las diferentes industrias con el fin de también buscar un desarrollo sustentable con el medio ambiente, combatiendo así el cambio climático. En definitiva, estos programas de investigación son la vía correcta para dar solución a las faltas de regulación dentro del IoT en Europa, debido a que mientras más se desarrolle la tecnología, más rápido podremos dar con las respuestas a las

[3] Horizon Europe es un programa de innovación creado por la Unión Europea en el año 2020 que, como se mencionó, lo que busca es una investigación, innovación y desarrollo de nuevas tecnologías emergentes, pero no solo en el ámbito del IoT, sino que también busca luchar contra el cambio climático, impulsar la competitividad y el crecimiento dentro de la Unión y facilitar la colaboración reforzando el impacto de la investigación y la innovación a la hora de desarrollar, apoyar y aplicar las políticas de la UE. Más información en https://research-and-innovation.ec.europa.eu/funding/funding-opportunities/funding-programmes-and-open-calls/horizon-europe_en

[4] En términos de industria de agricultura, el programa Horizon en su grupo 6 llamado "Alimentación, bioeconomía, recursos naturales, agricultura y entorno" busca digitalizar este sector industrial en la UE.

[5] El DG Connect es la actual responsable de que esta agenda europea de digitalización se lleve a cabo, apoyando proyectos digitales como los del programa Horizon Europe. Más información en https://commission.europa.eu/about-european-commission/departments-and-executive-agencies/communications-networks-content-and-technology_en

vulnerabilidades al derecho a la privacidad y seguridad que estos dispositivos puedan generar en las personas.

1.2. La regulación a la privacidad en España

En el Derecho Español la regulación de la privacidad nace desde la misma Constitución, la cual reconoce expresamente en el artículo 18 el Derecho a la privacidad, incluyendo, dentro de este articulo 4 esferas:

1. Primero que nada, se garantiza el derecho al honor, la intimidad personal y familiar y la propia imagen, lo que conocemos en nuestro país como el Derecho a la honra.
2. En segundo lugar, se garantiza la inviolabilidad del domicilio
3. En tercer lugar, el secreto de las comunicaciones, en las cuales se considera las postales, telegráficas y telefónicas.
4. Por último, solo la ley limita el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos (Constitución Española, 1978)

El numeral 4 es el que es de nuestro interés, ya que en él se regula la informática con el fin de garantizar la intimidad personal y familiar, este numeral vendría siendo el Derecho a la intimidad digital y protección de datos, haciendo una diferenciación del derecho a la intimidad, visto de una forma más general que se desarrolla en los puntos anteriores, que podríamos definirlo "como la esfera de protección que rodea la vida más privada del individuo frente a injerencias ajenas, con la salvedad de los supuestos previstos en la ley" (Lopez, 2013:p 584). Estos derechos son el punto de partida para llegar a la regulación, pero hay que tener en cuenta que ambos derechos definidos anteriormente se diferencian de lo que podríamos considerar como Derecho a la privacidad que "podría incluir a todos los datos referidos al individuo, sean o no de carácter sensible" (Lopez, 2013: p. 586).

A pesar de estas diferencias entre ambos derechos, no son ni por mucho menos incompatibles entre sí, razón por la cual se encuentran en la Constitución española de 1978

juntos en el artículo 18.1 y en el artículo 18.4, tal como lo menciona el tribunal constitucional español en la sentencia STC 292/2000 al decir que "el objeto de protección del derecho fundamental a la protección de datos no se limita sólo a los datos íntimos de la persona, sino a cualquier tipo de dato personal, sea o no íntima, el conocimiento o el uso de la cual por parte de terceros pueda afectar sus derechos, sean o no fundamentales, porque su objeto no es sólo la intimidad individual, que para lo cual está la protección que el art. 18.1 CE otorga, sino los datos de carácter personal. Por consiguiente, también afecta aquellos datos personales públicos, que, por el hecho de serlo, de ser accesibles al conocimiento de cualquier, no escapan al poder de disposición del afectado porque así lo garantiza su derecho a la protección de datos" (STC 292/2000: FJ °5).

Zanjado el tema semántico entre ambos derechos, pasamos a mencionar que España es uno de los países en Europa en el cual existe más avance en el tema de regularización de derecho a la privacidad digital, partiendo desde el RGPD de la UE del que hablamos en el apartado anterior, que da el pie de inicio a la regulación nacional española en términos de protección de la privacidad digital, creándose en base a este reglamento la Ley Orgánica de Protección de Datos y Garantía de los Derechos Digitales de 2018 (Desde ahora LOPDGDD), la cual es la adaptación en el Derecho interno de la RGPD, por lo que seguiría las mismas directrices del reglamento 2016/679 de la UE, dando una base legal sólida para regular el tratamiento de los datos personales por parte de las empresas, esta ley es una actualización de la antigua Ley Orgánica de Protección de Datos 15/1999 de 1999, que a su vez esta influenciada por la antigua directiva 95/46 de la UE de 1995, por lo que los avances en España están extremadamente ligados a los avances de las regulaciones a nivel europeo.

Los principales puntos de la LOPDGDD son los siguientes:

1. Debe existir consentimiento expreso y verificable por parte de los usuarios (Articulo 6), en el caso de los menores de edad solo existe consentimiento desde los 14 años en adelante (Artículo 7)
2. La obligación de dar información a los interesados (Artículo 11), dentro de los cuales se encuentran los derechos de acceso (artículo 13), rectificación (artículo 14), supresión

(artículo 15), limitación del tratamiento (artículo 16), portabilidad y oposición (artículos 17 y 18)

3. Asegurar la confidencialidad de la información obtenida (Artículo 5)

Por último, es importante mencionar que esta ley orgánica adapta también la comunicación de brechas de seguridad, las cuales se deben comunicar a los afectados y a la Agencia Española de Protección de Datos en un plazo máximo de 72 horas, como también el articulo 34 crea la figura del delegado de protección de datos, siendo esta parte de la ley más precisa que la regulación general europea, porque dice en específico que entidades deben poseer obligatoriamente un delegado de protección de datos, siendo algunos de estas entidades los colegios, los centros docentes, los establecimientos financieros, las entidades que exploten redes y presten servicios de comunicaciones electrónicas y los prestadores de servicios de la sociedad de la información cuando elaboren a gran escala perfiles de los usuarios del servicio (Art 34, LOPDGDD 3/2018, 5 de diciembre). Este último es importante mencionarlo porque estos prestadores de servicios de la sociedad de la información pueden ser empresas de big data, por lo que su estricta regulación y que tengan a alguien a cargo de la protección de datos es fundamental para que no vuelvan a suceder casos como el de Cambridge Analytica[6], la cual fue protagonista del mayor escándalo de vulneración de la privacidad y de datos personales de la última década. (BBC Mundo, 2018)

1.3. El Internet de las cosas en España

España fue uno de los primeros países en el que se comenzó a desarrollar la tecnología del IoT, con la aparición de pequeñas empresas relacionadas con el Internet de las Cosas desde 2005, pero realmente la diferencia se marca desde el año 2010 en adelante cuando "comenzó a constatarse un auge por las ciudades inteligentes en España que conlleva el nacimiento de la RECI (Red Española de Ciudades Inteligentes)" (Vega et al, 2015: p. 31). La RECI es formada

[6] Cambridge Analytica era una empresa británica que usaba el análisis de datos para desarrollar campañas para marcas y políticos, la cual durante la década pasada se vio envuelta en un caso de vulneración de datos personales, que consistió en recopilar datos por medio de prueba de personalidad, entre otros, en la red social Facebook. Aquellos datos posteriormente fueron vendidos para influir en campañas políticas, siendo la más importante la elección a la presidencia de Estados Unidos de Donald Trump el año 2016

por ciudades de 50.000 habitantes en adelante, partiendo con 27 de las ciudades más grandes de España en el año 2012, pasando a tener 81 miembros en 2017, a 89 ciudades a 2022, el objetivo mencionado por ellos es el de "intercambiar experiencias y trabajar conjuntamente para desarrollar un modelo de gestión sostenible y mejorar la calidad de vida de los ciudadanos, incidiendo en aspecto como el ahorro energético, la movilidad sostenible, la administración electrónica, la atención de personas o la seguridad"(RECI, 2012).

También es importante destacar que, en el mismo año 2012, el Instituto de Diversificación y Ahorro de la Energía, dependiente del Ministerio de la Industria, Turismo y Comercio, atribuye a las ciudades inteligentes tres características:

- No dañar el medio ambiente
- Usar las tecnologías de la información y las comunicaciones como herramientas para la gestión
- Asumir como fin último el desarrollo sostenible (Bouzas R. and López B., 2015: p. 4)

Finalmente, las ciudades inteligentes españolas también se apoyan en la Red de Iniciativas Urbanas, también llamada RIU, el que según Moreno "cuenta entre sus objetivos facilitar la integración de las tecnologías de la información y comunicación en el desarrollo urbano, avanzando hacia un modelo de ciudad inteligente" (Moreno, 2018: p. 31), por lo que el desarrollo de las ciudades inteligentes en el país ibérico va a pasos agigantados en comparación a nuestro país.

En cuanto a otros ámbitos de la tecnología IoT, en España esta tecnología fue surgiendo de manos de la alta demanda académica en cuanto a temas de investigación, de ahí surgieron empresas enfocadas en guardar datos en la nube enfocados en investigaciones académicas, este temprano desarrollo ha ayudado a que "la reputación internacional de España en el sector del IoT fuera notoria y que el país cuente con empresas que son referencia a nivel mundial, teniendo como actores principales a operadores Wifi que han dotado al país de la conectividad inicial necesaria en determinados puntos como en plazas, aeropuertos y otros lugares de interés general" (Vega et al, 2015: p. 32). Se espera que este crecimiento de empresas dedicadas al IoT vaya en aumento a medida de los años y que no solo se enfoque en ciertos aspectos

Finalmente es importante que nos refiramos a un estudio de caracterización del uso de dispositivos IoT en la población española, que fue realizado durante 2021 el que nos muestra los

diferentes usos que se le da al IoT en España, qué grupos etarios son aquellos que le dan más uso al Internet de las cosas y que dispositivo electrónico relacionado a la tecnología es el más popular. Según el estudio, en España un 85% de las personas conoce dispositivos con la tecnología IoT, el cual al dividirlo por rangos etarios, da por resultado que el rango etario que más conoce sobre los dispositivos o sistemas conectados a Internet es el rango de 35 a 44 años de edad con un 22.37%, seguido de las personas de 45 a 54 años de edad con un 22.19%, algo que sorprende, ya que se podría pensar que los rangos etarios que más conocen sobre estas nuevas tecnologías son las nuevas generaciones que han convivido con el Internet desde que han nacido, pero este rango etario que va desde 16 a 24 años es el segundo que menos conoce los dispositivos del IoT, con solo un 14.16%(Quintana, 2021: p. 22).

En cuanto a los dispositivos que más se ocupan en el país, son los asistentes virtuales de voz como lo son Alexa de Amazon, Siri de Apple, Google Home, con un 18.1% de las preferencias, siendo alrededor de 5.941.055 de personas los que han utilizado alguna vez estos dispositivos, lo que es consecuente con lo que observamos en el capítulo anterior respecto al análisis de mercado hecho por la Comisión Europea. Luego, en segundo lugar, tenemos a los electrodomésticos conectados a Internet con un 10.8%, los sistemas de seguridad del hogar con un 9.5% y finalmente, los sistemas para la administración de energía con un 8.4% (Quintana, 2021: p. 23).

Esto nos deja como conclusión de que el IoT en España se ha desarrollado a pasos agigantados producto de un crecimiento de industrias que han comenzado a apostar por esta tecnología a principios de siglo cuando recién se estaba creando formalmente como tal, además de la creación de una gran red de ciudades que actualmente están apostando por formar más ciudades inteligentes a lo largo del país, además de una correcta regulación de estas nuevas tecnologías, gracias a la guía de la Unión Europea, produciendo que las leyes para evitar vulneraciones a la privacidad por medio de la tecnología sean menores y tengan sanciones a quienes las incumplan.

1.4. La regulación y el avance del IoT en el Reino Unido

Al igual que en el resto del continente, en el Reino Unido el avance del IoT ha llegado a pasos agigantados, un ejemplo de esto es que a finales de 2020 "aproximadamente existían 53 millones de metros *inteligentes*[7] desplegados en las casas del Reino Unido"(Noto La Diega, 2016: p. 81). Por esto, el gobierno lo que busca es proteger a los consumidores frente a las amenazas a la privacidad que podría suponer, es por esto que desde casi la mitad de la década de 2010, el gobierno británico ha tratado de impulsar y regular el Internet de las cosas, desarrollando inversión pública para que este sector del Internet crezca, como en 2015 que "el gobierno británico anuncio una inyección de recursos a la industria del IoT de 40 millones de libras esterlinas para enfocarse en la industria de la salud, cuidados sociales y ciudades inteligentes" (Ofgem, 2015).

En cuanto a regulación del IoT, el primer acercamiento a la regulación de parte del gobierno de Reino Unido fue en el año 2014, con el *IoT Blackett Review* realizado por el *Uk Government Chief Scientific Advisor* que recomendó que "la legislación debería mantenerse en los mínimos requeridos para facilitar el avance del Internet de las Cosas" (Tanczer et al., 2019: p. 41), esta publicación fue fundamental para que el Reino Unido comenzara una política de regulación flexible para no quedarse atrás frente al cambio tecnológico, como también de inversión como se mencionó anteriormente, junto con la creación de la IoTUK en 2015, el cual fue un programa de 3 años que informaba sobre los avances del IoT en el país, siendo parte de la inversión que hizo el gobierno.

Posteriormente, en 2018 en base a la regulación de la Unión Europea (en ese tiempo UK aun formaba parte de la Unión Europea), se creó por parte del Department for Digital, Culture, Media & Sport el *Code of Practice for consumer IoT security* el cual a propias palabras de este contiene "lo que se consideran buenas prácticas en la seguridad del IoT" (DDCMS, 2018), dentro de las decisiones que toman para mejorar la seguridad de la tecnología se encuentran las siguientes:

1. No existirán contraseñas por defecto en los dispositivos: Esto significa que los dispositivos electrónicos que tengan la tecnología de IoT no vendrán con un clave por

[7] Los metros Inteligentes, o Smart Meters en inglés, son dispositivos de monitorio y supervisión de la energía para la visualización de datos y generación de informes eléctricos, estos otorgan un seguimiento en tiempo real de las condiciones de la alimentación eléctrica. Más información en https://wenuwork.cl/iot-versus-smart-meters-ventajas-y-desventajas/#:~:text=Los%20Smart%20Meters%20son%20dispositivos,y%20generaci%C3%B3n%20de%20informes%20el%C3%A9ctricos.

defecto de fábrica, por lo que otros medios serán necesarios para autentificar los productos.

2. Las empresas que brinden dispositivos y servicios conectados a Internet deben proporcionar un punto de contacto o algún número que sea público para que se divulguen las vulnerabilidades de seguridad de sus productos, todo esto para que se pueda actuar de una manera rápida y para corregir estas vulneraciones de seguridad.
3. Tener actualizaciones con menos intervalos de tiempo para que existan menos brechas de seguridad en los dispositivos

Este código de prácticas tenía como rango de aplicación a la industria, la academia, organizaciones de consumidores y otros departamentos de gobiernos internacionales. Luego, en enero de 2020, se publicó una respuesta por parte del ministerio a una consulta abierta para mejorar este código, el cual comenzó a gestarse en mayo de 2019 y concluyó en junio de ese mismo año, se buscaba un feedback de parte de las empresas que se estaban regulando y el impacto que las propuestas de regulación habían generado durante estos 2 años de aplicación. (DDCMS, 2020: pp. 3-7)

Finalmente, debemos mencionar que el Reino Unido antes del Brexit se encontraba regulado también por el reglamento 2016/679, conocido como el RGDP, de forma general, a través de *the data protection act 2018*, el cual es la implementación de este reglamento de la UE en el país. Sin embargo, con el Brexit se entiende de que el RGDP no aplica más en el Reino Unido, dando la situación de que el reglamento ya no es válido para la regulación, pero el RGDP sigue contenido dentro de la ley británica dentro del *data protection act*, mencionado anteriormente, siendo esto un total retrocedo en materia de regulación del derecho a la privacidad en Internet.

2. Estados Unidos

2.1. Regulación del IoT en USA

Como bien se habló en el apartado sobre la Unión Europea, en el cual se mencionó que la regulación al Internet de las cosas comenzaba desde un plano de desconfianza en las empresas en términos de utilización de datos, lo contrario sucede en Estados Unidos, en que según Feldgen "a los estadounidenses les preocupa más que su gobierno invada su privacidad. Siendo, mas importante tener libertad para lograr sus objetivos y ejercer el derecho a elegir que el Estado asegure las necesidades básicas de todos los ciudadanos, considerando que la regulación es incompatible con la innovación"(Feldgen, 2018: p. 31). Esto da por consecuencia que hasta el año 2020 no exista una normativa federal para todo Estados Unidos. En ese año se promulgó la *Public Law No: 116-207,* también llamada *Internet of Things Cybersecurity Improvement Act of 2020"*[8] la cual describe "los requisitos de seguridad que deben cumplir en el futuro los dispositivos de propiedad o controlados por el gobierno federal que estén conectados a sus sistemas informáticos"(Roberts y Weidenslaufer, 2021: p. 4). Esta ley parte definiendo lo que es el IoT, al señalar que es "Una extensión de la conectividad del Internet a dispositivos físicos y toda clase de objetos cotidianos" (Gibson Dunn, 2021), lo que causa curiosidad porque esta definición excluye a los aparatos electrónicos convencionales como los computadores, los celulares inteligentes o las tabletas. (Roberts y Weidenslaufer, 2021: p. 4)

Esta ley según el estudio jurídico Gibson Dunn lo que hace es otorgarle poderes a la *National Institute of Standard and Technology* (Desde ahora NIST), para desarrollar estándares de seguridad y pautas para un uso y manejo apropiado de todos los dispositivos IoT que tengan el gobierno federal y estén conectados a sus sistemas de información (Gibson Dunn, 2021). También el NIST "debe revisar y actualizar sus estándares cada 5 años para mantenerse al día respecto de nuevas preocupaciones con relación a los datos obtenidos"(Roberts y Weidenslaufer, 2021).

[8] Ley de mejora de la seguridad cibernética de IoT de los EE. UU. en español

También según la sección 4 a 2 del Act 2020, el NIST debe ser consistente de los esfuerzos con respecto a posibles vulnerabilidades de la seguridad del IoT, y además debe seguir las siguientes consideraciones respecto a los dispositivos que tengan IoT

1. Que tengan un desarrollo seguro
2. Gestión de identidad
3. Parches
4. Manejo de configuraciones

Además, debe considerar estándares, pautas y mejores prácticas relevantes desarrolladas con el sector privado, agencias y asociaciones público-privadas (Public law N° 116-207, sección 4 a 1 y 2, 2020)

Finalmente, también debemos de mencionar que, desde el 5 de diciembre de 2022, todas las agencias gubernamentales no pueden renovar los contratos de adquisición con empresas cuyos dispositivos de IoT no cumplan con los estándares y directrices del NIST, esto de acuerdo con la sección 7 (a)(1) y la sección 7 (d) de la misma ley que indica que todas las prohibiciones mencionadas en la ley tendrán efecto desde 2 años de publicada, cumpliéndose en la fecha mencionada anteriormente. (Public law N° 116-207, sección 7 a 1 y sección 7 d, 2020)

Saliendo de la ley a nivel federal en el país norteamericano, es importante que hablemos de la primera ley a nivel estadual que regula la privacidad de la información en Internet, que es la *California´s law N° 327, 2018*, la cual fue promulgada en 2018, pero su entrada en vigor fue el día 1 de enero de 2020, considerada por muchos autores como un hito a la regulación del IoT en Estados Unidos. Esta ley es importante por el contexto histórico y geográfico en del estado de California, siendo este estado "la Meca" de la tecnología desde finales del siglo pasado, siendo el lugar de ubicación de Silicon Valley, siendo aquel lugar en el cual se encuentran las bases de operaciones de las empresas más grandes del mundo tecnológico como lo son Facebook, Google, Apple, por lo que se hace evidente y necesaria una regulación que estableciera estándares de seguridad mínimas para los dispositivos conectados a Internet.

La ley de California fue agregada a la parte 4 de la división 3 del Código Civil del mismo Estado, siendo importantes artículos como el 1798.91.04. (a) que obliga a los fabricantes de dispositivos que se conectan a Internet equipar características de seguridad razonables, las cuales son las siguientes:

1. Que sean apropiadas para la naturaleza y la función del dispositivo
2. Que sean apropiadas para la información que recolectan, contienen y trasmiten
3. Que sean diseñadas para proteger al dispositivo y a cualquier información contenida de accesos no autorizados, destrucción, uso, modificación y divulgación (SB/327, 1798.91.04 a, 2018)

Luego, en el apartado b), la ley exige que todo dispositivo conectado fuera de una red de área local sea equipado con un medio de autentificación con una característica de seguridad razonable. También que la contraseña que venga por defecto sea única para ese dispositivo y que el dispositivo contenga una función de seguridad que requiere que un usuario genere un nuevo medio de autentificación antes de otorgarle acceso al dispositivo por primera vez (SB/327, 1798.91.04 b, 2018)

Para concluir con esta regulación, es necesario decir que existen detractores a esta normativa, como el experto en ciberseguridad Robert Graham, quien afirma que la ley es "típicamente mala, pues se basa en una comprensión superficial de la ciberseguridad y la piratería, que va a haber poco para mejorar la seguridad y hace mucho para imponer costos y dañar la innovación"(Porcelli, 2020: p. 18), argumentando igualmente que tratar de solucionar los problemas con parches o actualizaciones constantes en los dispositivos no es una solución, porque no hay certeza de que las empresas de Internet den a los consumidores tales parches, o peor aún, que los consumidores actualicen los dispositivos, sobre todo en dispositivos que no sean teléfonos, tablets o computadoras, ya que estos simplemente se instalan en los lugares en que se van a ocupar y los usuarios "no ven las notificaciones o no se notifican a los usuarios correctamente sobre la aplicación de parches" (Porcelli, 2020: p. 19)

Para terminar, podemos concluir que Estados Unidos está recién entrando en el camino de la regulación del Internet de las Cosas, regulando primariamente a las empresas en términos de seguridad, pero aún falta regular cosas básicas como el consentimiento de la entrega de la información de parte de los consumidores, la trasparencia sobre el uso de la información, y que las agencias reguladoras puedan sancionar a las empresas en caso de omisiones a la ley.

Conclusiones

Como hemos expuesto, si bien en nuestro país se ha visto una preocupación por mejorar y actualizar su regulación en torno a la protección de datos y la aparejada protección a la privacidad de las personas, la tardía función legislativa que se ha dado en cuanto a la modificación de esta normativa ha obstaculizado el surgimiento de un modelo eficaz de regulación en este tema. Lo anterior nos parece preocupante ya que el avance de la tecnología es mucho más acelerado que los procesos legislativos por lo que incluso si el día de mañana se logra por fin aprobar un proyecto de reforma en torno a derechos digitales, será altamente probable que este quede desactualizado rápidamente en unos cuantos años quedando en riesgo nuevamente la protección de la vida privada de las personas.

En primer lugar, esto lo vemos reflejado en el actual proyecto de ley que modifica la actual ley 19.628. El proyecto si bien propone diversas modificaciones, añade nuevos conceptos y crea diferentes instituciones como la Agencia de Protección de Datos Personales y el Registro Nacional de Cumplimiento y Sanciones, aún presenta falencias al no contemplar realmente la magnitud del desarrollo tecnológico y de la Internet enfocándose en utilizar como base de su regulación las centrales de tratamiento de datos vistas como industrias o instituciones, sean públicas o privadas, especializadas en la recopilación y el tratamiento de la información personal, cuando la realidad es que todo nuestro entorno está constantemente recopilando nuestra información personal ya sea por ejemplo mediante redes sociales o dispositivos electrónicos que se van adaptando a nuestras necesidades y preferencias para esta recolección de información.

En segundo lugar, a pesar de las carencias que podemos tener como país en términos de regulación, es importante mencionar que no solo es un problema nuestro, sino una problemática global al avance de la tecnología como mencionamos anteriormente, de acuerdo con las legislaciones analizadas, la única legislación que realmente se actualiza de manera uniforme y correcta era la vigente en la Unión Europea, la cual otorga herramientas adecuadas para sancionar a las empresas que incurren en malas prácticas y afectaciones al derecho de la privacidad, además de que se pone enfoque en el consentimiento de las personas para dar entrada al tratamiento de datos personales, algo que en otras regulaciones, como la de nuestro país, aún no se da en la

práctica. También, podemos decir que el modelo estadounidense de regulación presenta falencias al solo enfocarse en los dispositivos que utiliza el gobierno federal, básicamente siendo una regulación que busca controlar el tratamiento de datos personales y de la privacidad de las personas provenientes del Estado, no siendo controladas las actuaciones de empresas en el país.

Esto último llega a ser muy perjudicial, ya que, en su mayoría, las empresas más grandes del mundo con relación al IoT son de origen estadounidense, en consecuencia, el no regular correctamente las empresas que afectan nuestra privacidad y datos personales, no solo daña al país norteamericano, sino que a todo el mundo. Un ejemplo de esto es, como todos sabemos, son las decisiones políticas de Estados Unidos, y como bien se sabe, se manipularon los datos personales para una elección presidencial[9], dando al mundo una señal de que es posible lograr una victoria electoral por medio del control de datos, más aún si no existe regulación de por medio que logra impedirlo.

En tercer lugar, nuestra propuesta para mejorar la aplicación de la regulación al IoT en nuestro país es comenzar con mejorar las herramientas de solución de controversias que actualmente rigen en nuestro derecho, siendo necesario que se dé una mayor importancia al Derecho de Acceso o Habeas Data consagrándolo como una garantía constitucional y una acción de amparo distinta del Recurso de Protección con la finalidad de una mayor autodeterminación de los derechos personales y una eficaz protección del derecho a la privacidad sin la necesidad de que el acto sea ilegal o arbitrario.

Asimismo, para lograr esta eficacia y eficiencia de la reglamentación, el camino a seguir en general debe ser ampliar lo mayor posible su ámbito de aplicación tanto para la clase de personas que pretende proteger como para los tipos de datos que se tratan, así como las fuentes desde las cuales se recopilan estos datos y finalmente se almacenan teniendo como límite el derecho a la información. Es fundamental lograr una buena aplicación de los derechos ARCOPI cuando la nueva ley de protección de datos personales se promulgue, y que, desde luego, se considere el consentimiento expreso de las personas como un requisito primordial para que las

[9] La elección de 2016 de Donald Trump fue afectada por campañas políticas enfocada en ciertos sujetos por los datos obtenidos que Facebook no protegió en su momento, logrando así la victoria del político a la presidencia de Estados Unidos, como se mencionó anteriormente con el caso de Cambridge Analytica.

empresas puedan manipular los datos personales de las personas. Para así, en caso de incumplimiento de la ley por parte de estas, la pretendida Agencia de Protección de Datos Personales pueda cumplir sus funciones, entre ellas la libertad de investigar estos casos y de sancionar de manera efectiva a las empresas, no así como ocurre actualmente con instituciones de otros ámbitos, como es el caso del SERNAC en el derecho del consumidor, el cual no posee facultades sancionatorias.

En cuarto lugar, es indispensable aplicar un modelo preventivo en nuestro país, que obligue a las empresas que venden dispositivos conectados al IoT cumplir unos estándares mínimos de seguridad en términos de privacidad, como obligar a las empresas que sus dispositivos tengan una contraseña por defecto que sea única de este, mantener actualizaciones constantes en sus softwares para evitar robo de datos, tener un número de teléfono o una página web en funcionamiento para que se informe de cualquier situación de vulnerabilidad, entre otros. Con la sanción de prohibir a las empresas de comercializar sus dispositivos en caso de no cumplir con alguno de estos estándares.

Finalmente, es necesaria una mayor inversión en investigación y desarrollo de la tecnología del IoT, siendo esta otra solución plausible para lograr una mejor regulación, ya que, mientras más conocimiento exista sobre el IoT, es posible que se puedan llegar a nuevos y mejores modelos regulatorios, creación de nuevas agencias reguladoras, entre otros, que impidan la afectación de la privacidad y los datos personales que existen dentro de las nubes de las empresas del IoT. Este desarrollo, desde luego conlleva a otros beneficios que nos puede dar el IoT, uno de ellos es la mejor conectividad y mayor seguridad dentro de las ciudades, siendo esto uno de los objetivos de las ciudades inteligentes. Pero el más importante de todos es posiblemente el permitirnos ser más sustentables medioambientalmente, siendo esto indispensable en la lucha contra el cambio climático, por lo que el IoT será parte fundamental del futuro de la humanidad dentro de las próximas décadas.

Si bien el Internet de las cosas puede parecernos un tanto invasivo en nuestra esfera de privacidad teniendo en cuenta todo lo anterior planteado, esto no debe suponer una amenaza para el derecho a la privacidad siempre y cuando se regule de manera eficaz y efectiva, respetando el debido procedimiento de recopilación y tratamiento de los datos personales, utilizándolos con

el debido fin para el cual se almacenan y utilizando como base principal el consentimiento informado de los titulares.

Bibliografía

Barrio, A. (2020). *"El Internet de las cosas"*, Reus, Madrid

Bobadilla, Á. M. (2020). Los derechos digitales en Europa tras la entrada en vigor del Reglamento de Protección de Datos Personales: un antes y un después para el Derecho al olvido digital. *Revista de Estudios Constitucionales*, *18*(2), 121–150. Disponible en: https://doi.org/10.4067/s0718-52002020000200121

Bouzas R., & López B. (2015). *Smart City Y Gobernanza: Elementos Catalizadores y Desarrollo de la Democracia. El Caso de la Red Española de Ciudades Inteligentes*. Disponible en http://data.worldbank.org/indicator/SP.URB.TOTL.IN.ZS

Corral, H. (2000). Configuración jurídica del derecho a la privacidad I: Origen, desarrollo y fundamentos. *Revista Chilena de Derecho*, *Vol. 27 N° 1*, 51–79.

Corral, H. (2000). Configuración jurídica del derecho a la privacidad II: Concepto y delimitación. *Revista Chilena de Derecho*, *Vol. 27*, 331–355.

Cortez, C. (2014). *El "Internet de las cosas": Más Internet que otra cosa*. Centro de Estudios en Libertad de Expresión y Acceso a la Información (CELE), Buenos Aires

Cruz, M., Oliete, P., Morales, C., González, C., Cendón, B., Hernández, A. (2015). *Las Tecnologías IoT dentro de la industria conectada 4.0*. Fundación EOI. Madrid

Espejo, C. (2018). *Estudio de las aplicaciones de la tecnología RFID y su grado de implantación*. Universidad de Sevilla

European Commission. (2022). *Sector inquiry into consumer Internet of Things*.

European Commission. (2020). *Europe´s Internet of Things Policy* [en línea]. Traducción propia. Disponible en: https://digital-strategy.ec.europa.eu/en/policies/internet-things-policy [Ultima consulta en diciembre de 2022]

Evans, D. (2011). *Internet de las Cosas, como la próxima evolución de Internet lo cambia todo*, en Cisco Internet Business Solutions Group (IBSG).

Feldgen, M. (2018, July). "Internet de las Cosas" y los ciudadanos. *Tecnología & Sociedad*, *7*, 27–48.

Gallego, C. (2022). Internet de las cosas: La tecnología como aliada de la sostenibilidad. EAE Business School. Barcelona. Disponible en https://www.informeticplus.com/internet-de-las-cosas-la-tecnologia-como-aliada-de-la-sostenibilidad-eae-business-school#:~:text=Internet%20de%20las%20cosas%3A%20La,la%20sostenibilidad%20(EAE%20Business%20School)&text=El%20informe%20ofrece%20una%20visi%C3%B3n,nivel%20de%20Latinoam%C3%A9rica%20y%20Europa.

Herrera, P. (2016). El derecho a la vida privada y las redes sociales en Chile. *Revista Chilena de Derecho y Tecnología*, *5*(1), 87–112. Disponible en https://doi.org/10.5354/0719-2584.2016.41268

IoT Analytics (2022). *State of IoT 2022: Number of connected IoT devices growing 18% to 14.4 billion globally* [en línea]. Traducción propia. Disponible en https://iot-analytics.com/number-connected-iot-devices/ [Ultima consulta en diciembre de 2022]

Jervis Ortiz, P. (2015); Internet de las cosas y protección de datos personales, en *Revista Chilena de Derecho y Tecnología*, Vol. 4, Santiago de Chile

Lopez, J. (2013, March 20). Los códigos tipo como instrumento para la protección de la privacidad en el ámbito digital: Apreciaciones desde el Derecho español. *Revista de Estudios Constitucionales*, *2*, 575–614.

Manyika, J., Chui, M., Bisson, P., Woetzel, J., Dobbs, R., Bughin, J., & Aharon, D. (2015). *The Internet of Things: Mapping the Value Beyond the Hype*. Traducción Propia, disponible en www.mckinsey.com/mgi.

Mesías, L. O., & Viollier, P. (2021). Repensando el derecho al olvido y la necesidad de su consagración legal en Chile. *Revista Chilena de Derecho y Tecnologia*, *10*(1), 77–109. https://doi.org/10.5354/0719-2584.2021.56482

Moreno, C. (2018). Ciudad inteligente y ciudad sostenible. *Anavam.Com*, 29–37. Disponible en http://anavam.com/wp-content/uploads/2018/06/Art%C3%ADculo-JUN.pdf

Noto La Diega, G. (2016). Cloud of Things: Data Protection and Consumer Law at the Intersection of Cloud Computing and the Internet of Things in the United Kingdom. *Journal of Law & Economic Regulation*, volumen *9*, 69–93. Traducción propia.

OCDE. (2002). *Directrices de la OCDE sobre protección de la privacidad y flujos transfronterizos de datos personales*. Disponible en www.oecd.org/bookshop

OFGEM (2015). *Ofgem announces £62.8 million to deliver smarter energy network for consumer* [en línea]. Disponible en https://www.ofgem.gov.uk/publications/ofgem-announces-ps628-million-deliver-smarter-energy-network-consumers [consulta: 10 de diciembre 2022].

Porcelli, A. M. (2020). Un hito jurídico sobre Internet de las Cosas: la Ley de California n° 327 del año 2018 vigente a partir del 1 enero del 2020. *Revista Direito GV*, *16*(1). https://doi.org/10.1590/2317-6172201953

Quintana, C. (2021). *Caracterización del uso de dispositivos IoT en la población española*.

Red Española de Ciudades Inteligentes (2011). *¿Quiénes Somos?* [en línea]. Disponible en https://reddeciudadesinteligentes.es/sobre-nosotros/ [consulta: 13 de diciembre 2022].

Rivas, A., Meraz, C., Pineda, C., Carrera, C., Gómez, D., Gálvez, D., Vásquez, D., Pérez, É., Zumarán, G., Calzada, J., Rodríguez, J., Salcido, K., Galindo, L., Medina, M., Solano, M., Carrete, N., Bocanegra, N., Almaraz, O., Treviño, O., & Pizarro, R. (2022). *Ciudades inteligentes e Internet de las cosas: Propuestas y casos de uso Coordinadores* (J. Gabriel, R. Pizarro, J. Calzada, y Rodríguez M, Eds.; Primera Edición). Tecnológico Nacional de México.

Roberts, R., & Weidenslaufer, C. (2021). *Internet de las Cosas (IoT) Regulación federal de Estados Unidos y del Estado de California*.

Rose, K., Eldridge, S., y Chapin, L. (2015). *La Internet de las Cosas- Una breve Reseña*.

Rose, K., Eldridge, S., & Chapin, L. (2015). *Para entender mejor los problemas y desafíos de un mundo más conectado*. Centro de Estudios en Libertad de Expresión y acceso a la información

Rostión, I. (2015). Sobre la Ley de Protección de la Vida Privada: La importancia de una "fuente legal" y su aplicación en las Personas Jurídicas. *Revista Ius et Praxis*, *2*, 499–520.

Salazar, J., Silvestre, Y. (2019). *Internet de las cosas*. Disponible en http://www.techpedia.eu

Tanczer, L. M., Brass, I., Elsden, M., Carr, M., & Blackstock, J. (2019). *The United Kingdom's Emerging Internet of Things (IoT) Policy Landscape*. In R. Ellis & V. Mohan (Eds.), Rewired: Cybersecurity Governance (pp. 37–56). Hoboken, New Jersey. Traducción propia.

Vial, F. (2001). La ley N° 19.628 Sobre protección de datos de carácter personal y una visión general. *Cuadernos de Extensión Jurídica*. Vol. 5, pp. 23-37

Normativa y Jurisprudencia

Nacional

Chile. Ley 19.628 (1999), Sobre Protección de la Vida Privada. De 28 agosto. Disponible en https://www.bcn.cl/leychile/navegar?idNorma=141599&idVersion=2020-08-26

Corte Suprema Sentencia 11.256/2011

Corte Suprema Sala Tercera Constitucional. Sentencia Nº 22243-2015. Resolución nº 36142. 21 de enero de 2016.

Corte Suprema Sala Tercera Constitucional. Sentencia Nº 7148/2015. Resolución nº 142279, de 14 de septiembre de 2015

Proyecto de Constitución Política de la República. (2022)

Boletín N° 11.114-07 (2017), Refundido con Boletín 11.092-07 (2017). Sobre Proyecto de Ley que Regula la Protección y el Tratamiento de los Datos Personales y Crea la Agencia de Protección de Datos Personales, de 15 de marzo.

Internacional

España. Constitución Española (1978), *Boletín Oficial del Estado,* núm. 311, de 29 de diciembre.

Sentencia del Tribunal Constitucional español Rol 292/2000: FJ °4 (2000).

España. Ley Orgánica 3/2018, de Protección de Datos Personales y garantía de los derechos digitales, *Boletín Oficial del Estado,* núm. 294, de jueves 6 de diciembre.

Reglamento (UE) 2016/679, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE. *Diario Oficial de la Unión Europea,* núm. 119, de 4 de mayo de 2016.

Reino Unido. DDCMS. (2018). *Code of Practice for Consumer IoT Security*. Traducción propia. Disponible en https://www.gov.uk/government/publications/secure-by-design

Reino Unido. DDCMS. (2020). *Government response to the "Regulatory proposals for consumer Internet of Things (IoT) security" consultation*. Traducción propia.

Estados Unidos. SB-327 (2018). Information privacy: connected devices. De 28 de septiembre.

Estados Unidos. Internet of Things Cybersecurity Improvement Act of Disponible en: (2020). Consultado en diciembre, 2022