Universidad de Granada

Facultad de Derecho

Escuela de Doctorado Humanidades, Ciencias Sociales y Jurídicas

Escuela Internacional de Posgrado

Programa de doctorado en Ciencias Jurídicas

RETOS Y OPORTUNIDADES JURÍDICAS ANTE LA DIGITALIZACIÓN

Doctoranda María Mercedes Aramendía Falco

Director y tutor: José Luis Pérez-Serrabona González

Diciembre 2020

Editor: Universidad de Granada. Tesis Doctorales
Autor: María Mercedes Aramendía Falco
ISBN: 978-84-1117-024-6
URI: http://hdl.handle.net/10481/70461

ÍNDICE

SUMMARY

We have moved from the classic society, physical, offline, to the digital society, data, online, which is constantly deepening and involves challenges and opportunities for all: citizens, businesses, governments, civil society, academia, among other examples.

This change is often referred to as the Digital Revolution or the 4.0 Revolution, which is based on telecommunications, was leveraged by the convergence of technology, the Internet and electronic platforms; and finally, together with the great technological advances -such as *Big Data,* cloud storage, Internet of Things, Artificial Intelligence and *Blockchain,* generated what is called the digital transformation, with great economic and social impacts.

In this sense, this research began by referring to the various challenges and opportunities that digitization brings. Then it was analyzed about the telecommunications networks and the new regulatory paradigms that are presented. The legal bases and institutional design are very important in the face of this new reality, so reference is made to the examples of Spain and Uruguay. The radio-electric spectrum is a fundamental element for the deployment and development of telecommunications services, and therefore this subject is also discussed in depth, with emphasis on Spain and Uruguay. Various digital services and applications are provided over the telecommunications networks, which generate what is known as the digital economy.

In this new economy, new digital markets are developing and countries have responded in various ways with regulation. All of this, in addition to having economic impacts, also had social consequences, mainly on people's human rights.

Since the area of research has global impact and focused mainly on Spain and Uruguay, the studies were carried out mainly at the University of Granada, Spain, Cornell University, USA, and the University of Montevideo, Uruguay.

In view of the above said and of the great changes that have been and continue to be generated, it is increasingly important that legal systems be reviewed in order to adapt to new needs. We must leave without effect that which no longer reflects reality, adjust or modernize that which requires it, and finally dictate those rules that are necessary. Likewise, taking into account the speed with which this new reality is deepening, having flexibility and adapting, as well as attending to the fundamental principles, defending the

consumer and promoting competition, are presented as the fundamental bases on which to work.

More than ever, the constant dialogue between the different actors in the sector, the collaboration, as well as generating predictability, security and promoting innovation, attending to the function and not the medium, is fundamental for the satisfactory development and for attracting essential investments for the constant growth of the digital ecosystem.

Resources will generally be scarce; the essential thing is to prioritize based on the public policies that are defined, as well as to promote innovation, research and development, sharing knowledge.

ANTECEDENTES

El 13 de junio de 2016 presenté el Plan de Investigación, el cual se denominó ¨La Promoción y Defensa de la Competencia en el mundo "online y offline", y tal como surge del Informe de Dirección de fecha 29 de septiembre de 2016, se aceptó el Plan y se defendió.

El tema de la tesis doctoral luego pasó a centrarse en la conocida "economía colaborativa", procurando investigar sobre la temática, así como estar actualizada de las discusiones y soluciones que se fueran generando tanto a nivel nacional, como regional e internacional.

A medida que se avanzó en la investigación y que toda esta temática de gran actualidad no paró de evolucionar, el tema se amplió. El mundo digital presenta una nueva realidad, planteándo múltiples desafíos para todos, especialmente para el Derecho en tanto busca atender las relaciones humanas, siendo reflejo de la justicia y el equilibrio.

Tanto el tema original ¨La promoción y defensa de la competencia en el mundo online y offline¨, como el segundo planteado ¨La economía colaborativa¨, son partes de un mismo tronco general, el mundo digital, específicamente la economía digital.

Se considera que el punto de partida debe ser ¨el mundo digital¨ y los desafíos que el mismo plantea para el Derecho. Por lo que en la presente investigación se analizan "Los Desafíos Jurídicos ante la Digitalización".

En vista de lo expuesto, se solicitó el cambio de título de la investigación, lo cual fue aprobado por el Comité de Dirección de la Escuela de Doctorado de Humanidades, Sociales y Jurídicas el 3 de diciembre de 2019.

El área de la investigación es muy amplia. Sin perjuicio, se considera que dentro de este gran tema se puede subdividir en dos. Por un lado los derechos fundamentales de las personas ante esta nueva realidad, principalmente lo que respecta al derecho a la comunicación, sus límites, y el derecho a la protección de los datos personales; y por otro lado, la economía digital que tiene entre sus desafíos la promoción y defensa de la competencia en condiciones de igualdad, así como los nuevos modelos de negocios, como es la economía colaborativa.

La Fase 1 del Plan terminó en diciembre de 2016. Se reunió bibliografía general, se identificaron posibles problemas, discusiones, diferentes posiciones, se centró el tema, y se comenzó a generar el índice. Por la actualidad de la temática, constantemente se está consultando diversas fuentes en la materia, tales como manuales, publicaciones de organismos internacionales y nacionales de diversos países, revistas especializadas, blogs de opinión, diversos medios en donde catedráticos de prestigio manifiesten su opinión, así como otros autores cuyas consideraciones puedan aportar al objeto de estudio.

La fase 2 del Plan finalizó en febrero de 2018. Se analizó la bibliografía recolectada, se trabajó en las diversas partes de la investigación y se comenzó a desarrollar el cuerpo de la tesis, el cual se ha ido ajustando a medida que se va profundizando en el trabajo, así como el conocimiento en la materia, en línea con la evolución de la temática.

La fase 3 del Plan finalizó en julio de 2018. Teniendo un conocimiento profundo de la materia, del estado a nivel internacional, así como las discusiones, debates y diferencias que se plantean, se comenzó a desarrollar el contenido.

Vale destacar que en el año 2017 se comenzó a dar clases en el Máster de Derecho de la Universidad de Montevideo. En ese año se dictó junto con los Profesores Carlos Delpiazzo y Cristina Vázquez, ambos Catedráticos Grado 5 de Derecho Administrativo en Uruguay, el curso: "Telecomunicaciones y Sociedad de la Información". En el año 2018 se dictó el curso "Protección de Datos Personales Tributarios y Bancarios", junto con el Dr. Pablo Schiavi, y el curso "Desafíos jurídicos ante la Digitalización" con la Dra. Cristina Vázquez. En el año 2019 se dirigió el curso "Transformación Digital y el Derecho", también en la Universidad de Montevideo, y se comenzó a trabajar como Profesor Ayudante en la materia "Derecho informático y nuevas tecnologías" en el Máster de Acceso a la Abogacía en la Universidad de Nebrija, de España.

Además, tras el dictado de los cursos se coordinó la publicación de dos libros y además se escribieron artículos que fueron publicados.

El primer libro fue denominado "Estudios de Telecomunicaciones y Sociedad de la Información", coordinado juntamente con la Dra. Cristina Vázquez, publicado por la Universidad de Montevideo, año 2018.

El segundo libro fue denominado “Estudios sobre los Desafíos Jurídicos ante la Digitalización”. Fui coordinadora junto con la Dra. Cristina Vázquez, y coautora. Fue publicado por la Universidad de Montevideo, año 2019.

Además realicé dos publicaciones en el libro “Estudios de Información Pública y Protección de Datos Personales”, Tomo III, publicado por la Universidad de Montevideo, en el año 2018.

En el mismo sentido, también realicé una publicación de impacto en la Revista de “Derecho y Nuevas Tecnologías”, número 3, año 2020, publicado por La Ley Uruguay, denominado “Seguridad en la era Digital”.

Durante la fase 4, se siguió trabajando en el contenido, el cual, por la actualidad de la temática se continúa alimentando continuamente, a fin de otorgar coherencia, creatividad, buscando aportar activa y constructivamente a la academia.

En este sentido, interesa destacar que se recibió una beca por mérito por la Universidad de Cornell y entre agosto de 2019 y mayo de 2020 se realizó el Máster en Derecho, Tecnología y Emprendedurismo, lo cual fue autorizado como instancia de investigación en el exterior.

Asimismo, vale señalar que desde marzo de 2020 dirijo el Postgrado de Transformación Digital y el Derecho en la Universidad de Montevideo, al tiempo que dicto ciertas materias vinculadas con mi área de investigación.

Durante toda la investigación se procuró estar siempre actualizado de las novedades a nivel comparado e internacional, así como participar en diversas actividades relacionadas con la temática, tales como Congresos, Jornadas y otros eventos relacionados con la investigación.

De la misma forma, se buscó atender a las diversas soluciones que en algunos países y regiones se fueron adoptando, así como jurisprudencia que se generó en la materia, recomendaciones que se dictaron a nivel internacional, y opiniones de organismos y catedráticos que puedan contribuir activamente a la investigación.

Se parte de la base de que las nuevas tecnologías junto con las telecomunicaciones (*smartphone*, automatización, *blockchain*, *big data*, almacenamiento en la nube, entre otros ejemplos), impactan en nuestros hogares, trabajos, ciudades, gobiernos y

empresas; generando enormes cambios a gran velocidad y configurando la Cuarta Revolución Industrial, conocida como la Revolución Digital.

Ante esta realidad, resulta esencial comprender estos nuevos conceptos, a fin de poder afrontar los retos que se presentan y tomar decisiones en medio de la transformación digital que estamos transitando.

Se desarrollan los diversos temas procurando dar en primera instancia una visión cabal de la temática y luego comentar específicamente sobre la regulación de la temática en España y en Uruguay.

España interesa especialmente en tanto es el país en el que estamos trabajando. Asimismo, se ha seleccionado Uruguay dado que es el otro país en el cual se ha realizado la investigación, siendo un referente en Latinoamérica por los grandes avances que ha tenido en la materia. Finalmente, Estados Unidos también será considerado en algunos casos dado que la transformación digital impacta y requiere soluciones globales.

El enfoque multidisciplinario, así como el trabajo en conjunto entre actores de diversas ramas de especialidad, es cada vez más esencial para un análisis amplio de la temática.

La presente investigación busca aportar al análisis en cuestión. La temática es sumamente amplia y de actualización constante, por lo que se espera que este acercamiento, sirva de ayuda y de guía.

INTRODUCCIÓN

Hemos pasado de la sociedad clásica, física, offline, a la sociedad digital, de la información, online, la cual se profundiza constantemente e implica desafíos para todos.

La Revolución Digital comenzó con la gran evolución de las telecomunicaciones, la cual se apalancó con la convergencia tecnológico, con Internet y con las plataformas electrónicas; y finalmente, juntos con los grandes avances tecnológicos –como ser: *Big Data*, el almacenamiento en la nube, Internet de las Cosas, Inteligencia Artificial y *Blockchain*–, generó lo que se denomina la transformación digital, con grandes impactos económicos y sociales.

En esta nueva realidad en que vivimos, tenemos más libertades y derechos; pero también tenemos nuevos retos y desafíos, que necesariamente debemos identificar y afrontar para garantizar los derechos fundamentales de las personas y promover el desarrollo de la economía digital.

Ante este nuevo escenario, diversos organismos regionales y nacionales han desarrollado sus Agendas Digitales, reflejando diversos aspectos sobre los cuales necesariamente se debe trabajar para el adecuado desarrollo del mundo digital, permitiendo el desarrollo del ecosistema en su conjunto, siendo clave el marco jurídico y el rol de quienes diseñan las políticas públicas, así como de quienes regulan, controlan y aplican las normas.

Considerando los grandes cambios que se han generado y que se siguen generando, se ve cada vez más la importancia de que los ordenamientos jurídicos se revean a fin de adaptarse a las nuevas necesidades. Hay que dejar sin efecto aquello que ya no refleja la realidad, ajustar o modernizar aquello que lo requiera, y finalmente dictar aquellas normas que sí sean necesarias. Asimismo, teniendo en cuenta la velocidad con que esta nueva realidad se está profundizando, tener flexibilidad y adaptarnos, así como atender los principios fundamentales, defender al consumidor y promover la competencia, se presenta como las bases fundamentales sobre las cuales trabajar.

Más que nunca el diálogo constante entre los diversos actores del sector, la colaboración, así como generar previsibilidad, seguridad e impulsar la innovación, atendiendo la función y no el medio, es fundamental para el adecuado desarrollo y para captar inversiones imprescindibles para el adecuado desarrollo del ecosistema digital.

Las redes de telecomunicaciones, principalmente Internet, junto con el gran desarrollo de la tecnología y la convergencia, son esenciales para que la transformación digital se pueda desarrollar debidamente, en tanto son la espina dorsal sobre las cuales se despliega todo el ecosistema digital. Con todos los cambios que se han generado y que continuamente se están presentando, se presentan nuevos paradigmas regulatorios y diversos modelos de gobernanza.

En este sentido, en la presente tesis analizo:

- En primer lugar, la transformación digital: los retos y oportunidades.
- En segundo lugar, las redes de telecomunicaciones: los nuevos paradigmas regulatorios, las bases jurídicas de los servicios, ejemplos de diseños institucionales, la prestación de los servicios y el espectro radioeléctrico.
- En tercer lugar, los servicios y aplicaciones digitales, así como las nuevas tecnologías disruptivas. Se profundizará sobre la prestación de los servicios, la economía digital, la competencia, la inclusión financiera, las FINTECH y algunos ejemplos de usos.
- Finalmente, los derechos fundamentales y las nuevas tecnologías de la información. Se profundiza sobre la privacidad y los datos personales, haciendo énfasis en el Reglamento General de Datos Personales, el impacto que tiene en España y en Uruguay, luego se desarrolla sobre la Ley de Privacidad de California, y se establecen las principales diferencias y similitudes entre ambas normas. Posteriormente, se desarrolla sobre la Libertad de expresión y el acceso a la información, profundizando en los discursos de odio y en la moderación de contenidos. Consecutivamente, se trata sobre el Derecho de Autor, su protección jurídica tanto en España como en Uruguay, haciendo mención especial a los desafíos que los derechos de autor tiene en la era digital. Finalmente, se presenta sobre la seguridad en el mundo digital, se hace énfasis al marco de ciberseguridad en Uruguay y en España, y se cierra con consideraciones finales.

En cada uno de los puntos, se trata la temática de manera genérica y posteriormente se profundiza en la regulación de España y en la de Uruguay.

España interesa especialmente en tanto es el país en el que estamos trabajando y además siempre ha sido un modelo tomado como referencia en la regulación de

Uruguay. Por otra parte, se ha seleccionado Uruguay dado que es el otro país en el cual se ha realizado la investigación, siendo un referente en Latinoamérica por los grandes avances que ha tenido en la materia. Finalmente, Estados Unidos también será considerado en algunos casos dado que parte de la investigación se realizó en dicho país, es un referente en tecnología y además la transformación digital impacta y requiere soluciones globales.

Se comienza analizando sobre la digitalización y la transformación digital porque es la realidad en la cual nos encontramos y ante la cual se plantea el objeto de estudio.

Los retos y oportunidades que la digitalización conlleva son múltiples, debiendo analizarse y trabajarse sobre ellos de forma transversal. En este sentido, es fundamental planificar, para ellos las Agendas Digitales son un buen ejemplo de cómo, tanto a nivel regional, como nacional, los países van identificando las diversas áreas sobre las cuales deben trabajar, estableciendo objetivos y metas, que les permitan medir, controlar y ajustar aquello que sea necesario.

A continuación, se hace énfasis en la importancia del despliegue de redes de telecomunicaciones para poder universalizar el acceso y para que todos podamos ser parte de la transformación digital.

Las redes de telecomunicaciones son la espina dorsal, la base sobre la cual se construye la digitalización y la nueva realidad, pero el tipo de servicio varía, ya cada vez más todo va por Internet, generando nuevos paradigmas regulatorias, así como diversos niveles de gobernanza.

Es fundamental alcanzar el acceso universal en los servicios de telecomunicaciones, pero para que la universalización sea posible, se tienen que realizar grandes inversiones, siendo esencial el trabajo en conjunto de los diversos actores del sector, así como un marco jurídico que otorgue seguridad, reglas claras y previsibilidad para captar inversiones y promover el desarrollo.

Las bases jurídicas, el diseño institucional y la forma en que se prestan los servicios nos permite visualizar aspectos fundamentales sobre la regulación de la temática, otorgando seguridad jurídica y permitiendo identificar los diversos roles.

El espectro radioeléctrico es esencial para la prestación de los servicios de comunicaciones inalámbricas, así como para el desarrollo del Internet de las cosas. Como se desarrolla, el espectro radioeléctrico es un recurso natural, intangible,

compartido, limitado, escaso, que se divide en bandas de frecuencias, a través de las cuales se transmiten las ondas electromagnéticas de los servicios de comunicación inalámbrica. Es muy requerido y su demanda está en alza, siendo fundamental su compartición y coordinación, en tanto es necesario para el desarrollo de diversos servicios y aplicaciones, como ser: servicios de voz móviles, banda ancha móvil y fija, wi-fi, televisión para abonados, televisión digital terrestre, Internet de las Cosas, entre otros múltiples ejemplos.

Sobre las redes de telecomunicaciones se desarrollan múltiples servicios y aplicaciones digitales, que se brindan a través de diversos sistemas y plataformas electrónicas, así como nuevas tecnologías, que atienden diversas necesidades sociales y económicas.

Las plataformas electrónicas permiten prestar y comercializar diversos servicios y productos, en todo o en parte a través de Internet, cambiando la forma de consumir de los usuarios, generando gran impacto en todas las áreas de actividad y construyendo la economía digital.

Hay plataformas de diferentes formas y tamaños, que se desarrollan constantemente y que cubren las más diversas actividades, a modo de ejemplo: plataformas de publicidad en línea, mercados en línea, motores de búsqueda, redes sociales, medios de difusión de contenidos, plataformas de distribución, servicios de comunicación, sistemas de pago, plataformas dedicadas a la economía colaborativa.

Se generan nuevas industrias que nacen de la convergencia de dos o más industrias, a modo de ejemplo se general las FINTECH, consecuencia de la fusión de la tecnología con las finanzas, REGTECH, producto de la unión entre la regulación y la tecnología, así como LEGALTECH, resultado de aplicar la tecnología al Derecho y viceversa.

Para el desarrollo de estas plataformas, así como de esta innovación, la protección y garantizar la propiedad intelectual e industrial es clave; así como el desarrollo de un ecosistema que facilite y haga posible su desarrollo.

Como consecuencia del despliegue de las redes de telecomunicaciones y de las diversas plataformas digitales que ofrecen multiplicidad de servicios y productos por medios electrónicos, se generó la economía digital, la cual modificó muchos modelos de

negocios, así como la manera en que se relacionan las empresas con los clientes y con la competencia.

La economía digital tiene muchos beneficios para las sociedades y para la economía, en tanto las formas cambian buscando atender las necesidades de la sociedad; mas al mismo tiempo presenta múltiples retos.

Identificar debidamente los diversos aspectos que pueden llegar a ser vulnerados, es esencial para poder trabajar sobre los mismos y alcanzar seguridad jurídica, innovación, desarrollo, investigación e inversión.

Se destaca que el diálogo entre los diversos actores y el trabajo en conjunto entre especialistas de diversas disciplinas es fundamental, los cambios se producen cada vez más rápido impactando en todo y en todos. Asimismo, la regulación juega un rol muy importante, siendo básico que sea adecuada, que se revise y actualice de ser necesario, a fin de que atienda la realidad y las necesidades, que no limite sin reales argumentos, al tiempo que proteja a los usuarios, promueve y fomente la leal y sana competencia, al tiempo que otorgue seguridad jurídica para facilitar la innovación, el desarrollo y atraer inversiones.

En este sentido, se comenta sobre las nuevas regulaciones para el desarrollo del mercado digital, tanto en España como en Uruguay. En especial se desarrolla sobre los servicios de la sociedad de la información y el comercio electrónico, los aspectos tributarios, así como diversos aspectos de actualidad como son los pagos y el dinero electrónico, las monedas digitales y el financiamiento colectivo.

Por otra parte, si bien Internet y las nuevas tecnologías, han facilitado la creación de nuevos servicios y aplicaciones digitales, que han generado un ecosistema digital que borra fronteras, que refleja que vivimos en una comunidad internacional, que ofrece más acceso, que empodera a las personas, generando múltiples oportunidades. Por otra parte, se reconoce que el ecosistema digital tiene muchos riesgos y retos, principalmente en relación con los derechos humanos, los cuales deben ser respetados tanto en línea (*online*) como fuera de línea (offline).

En este sentido, se analiza sobre la privacidad y la protección de los datos personales, se profundiza en la libertad de expresión y el acceso a la información, haciendo énfasis en los discursos de odio y en la moderación de contenidos.

Consecutivamente, se trata sobre los Derechos de autor y los desafíos que la nueva era conlleva, y finalmente se desarrolla sobre la seguridad en la era digital.

Hay que empoderar a las personas, garantizarles la libre expresión, aumentarles la seguridad y la privacidad, así como promover el diálogo interdisciplinario, siendo primordial el trabajo en conjunto entre los diversos actores del ecosistema, tanto a nivel nacional, como regional e internacional.

Proteger la Privacidad y los datos Personales de las personales es clave, hay que buscar nuevas formas que permitan el adecuado uso de los datos sin vulnerar los Derechos Humanos. Son realmente interesantes las soluciones planteadas por el RGDP y la CCPA, sin duda normas innovadoras con impacto mundial.

Es esencial garantizar la libertad de expresión y el acceso a la información, al tiempo que considerar aquellas excepciones que sean necesarias, como puede ser el caso de los discursos de odio, así como la moderación de contenidos para poder disfrutar de una Internet libre.

Los Derechos de Autor impulsan a que las personas innoven, investiguen y desarrollen, pero es esencial protegerlos para que las personas puedan seguir teniendo protección y estímulos. La inteligencia artificial, la robótica, así como los nuevos desarrollos que constantemente se profundizan, desafían a los Derechos de Autor siendo esencial la actualización de los marcos para garantizar la protección al tiempo que se impulse la innovación.

La seguridad en la era digital es clave. No solo tiene impacto global, sino que es un factor clave para que las personas, empresas y organizaciones en general confíen, abracen cada vez más la tecnología, la digitalización, generando una cultura de prevención, que permita el efectivo goce, al tiempo que se proteja adecuadamente.

La ciberseguridad, así como la educación para que las personas puedan adquirir las nuevas habilidades digitales, es esencial para atender el futuro del trabajo, la inclusión social, la universalización de acceso, haciendo posible el logro de los Objetivos de Desarrollo Sostenible al 2030, aprobados por las Naciones Unidas en Setiembre de 2015.

Sin duda la digitalización conlleva un sinfín de retos y oportunidades, muchos de los cuales aún no los conocemos, evolucionan constantemente y es importante constantemente investigar, innovar, desarrollar, así como compartir el conocimiento

para poder generar las bases del desarrollo, permitiendo que todos seamos parte y que no quede nadie atrás.

CAPÍTULO I: LA DIGITALIZACIÓN: RETOS Y OPORTUNIDADES[1]

I. Introducción

Las Tecnologías de la Información y las Comunicaciones (TIC) impactan en toda la sociedad, tienen cada vez mayor participación en todos los ámbitos de nuestras vidas y tienen un rol clave para el desarrollo social y económico de todos, generando múltiples oportunidades y desafíos, que plantean al orden jurídico el reto de adaptarse y de responder adecuadamente al nuevo contexto.

Los hechos por sí solos nos dicen poco, tener en cuenta el contexto, todo el ecosistema, así como la historia y la evolución, es esencial para poder comprender y afrontar mejor cualquier situación.

Cuando hablamos de contexto, nos referimos al entorno físico o de situación, ya sea político, histórico, cultural o de cualquier índole en el que se considera un hecho o una determinada situación[2]. Cuando comenzamos a analizar un fenómeno, tener en cuenta los antecedentes, así como lo que está –o estaba– aconteciendo en ese momento y las diversas posiciones, nos ayuda a comprender de mejor forma toda la situación, alcanzando soluciones que reflejen la realidad y las necesidades.

Actualmente nos encontramos ante una nueva revolución, la digital, la cual comenzó con la gran evolución de las telecomunicaciones. Se apalancó con la convergencia tecnológico, con Internet y con las plataformas electrónicas; y finalmente, juntos con los grandes avances tecnológicos –como ser: Big Data, el almacenamiento en la nube, Internet de las Cosas, Inteligencia Artificial y *Blockchain*–, generó lo que se denomina la transformación digital, con grandes impactos económicos y sociales.

En esta nueva realidad en que vivimos, tenemos más libertades sociales, más beneficios, más opciones de elegir y más innovación, todo lo cual ha facilitado que las formas cambien. No solo ha variado la forma en que nos comunicamos, sino que también la manera en que nos relacionamos, en que trabajamos, en que estudiamos, en que nos transportamos, en que compramos, en que pagamos, entre otros variados ejemplos.

---

[1] Véase nuestro trabajo en ARAMEDIA, MERCEDES, "La digitalización: retos y oportunidades" en *Estudios Sobre los Desafíos Jurídicos ante la Digitalización*, Universidad de Montevideo, 2019, pp. 25 y ss.

2 Diccionario de la Real Academia Española, definición de Contexto, 2., URL: http://dle.rae.es/?id=AVBbFZW ◇ Consultado el 15 de enero de 2019.

Cada vez es más evidente que hemos pasado de la sociedad clásica, física, offline, a la sociedad digital, de la información, *online*, la cual se profundiza constantemente e implica desafíos para todos –personas físicas, jurídicas, gobiernos, sociedad civil, mercado, empresas, etc.–; los cuales necesariamente debemos identificar y afrontar para garantizar los derechos fundamentales de las personas, para alcanzar el acceso universal, conectar a todos, disminuir la brecha digital, actualizar y facilitar la educación, promover el despliegue de redes de telecomunicaciones de última generación, así como fomentar la innovación, el desarrollo y la competitividad, otorgando reglas claras, previsibles y seguridad jurídica.

Lo anterior es un fenómeno global, y más allá de que hay algunos países más avanzados que otros, ya muchas regiones y países han desarrollado sus agendas digitales, reconociendo la importancia que estos aspectos tienen para la sociedad y para la economía.

Los desafíos son múltiples, cabe destacar aquellos vinculados a los derechos digitales, a la regulación de las TIC y a la Gobernanza de Internet, así como lo relacionado al despliegue de redes, a los servicios y aplicaciones digitales, las plataformas electrónicas, la inclusión financiera, los activos digitales, la competencia, los derechos humanos, la privacidad, la libertad de expresión, el futuro de trabajo, entre otros múltiples ejemplos, muchos de los cuales se desarrollarán en las próximas páginas del presente libro.

Quiero comenzar haciendo referencia a una reflexión del libro "Homo Deus" de Yuval Noah Harari, la cual procedo a transcribir: *"Si pensamos en términos de meses, probablemente tendríamos que centrarnos en problemas inmediatos como los disturbios en Oriente Medio, la crisis de los refugiados en Europa y la desaceleración de la economía china. Si pensamos en términos de décadas, el calentamiento global, la desigualdad creciente y la disrupción del mercado laboral cobran mucha importancia. Pero si adoptamos una visión realmente amplia de la vida, todos los demás problemas y cuestiones resultan eclipsados por tres procesos interconectados: 1. La ciencia converge en un dogma universal, que afirma que los organismos son algoritmos y que la vida es procesamiento de datos. 2. La inteligencia se desconecta de la conciencia. 3.*

Algoritmos no conscientes pero inteligentísimos pronto podrían conocernos mejor que nosotros mismos.[3] *"*

Lo anterior converge en tres preguntas: *"1. ¿son en verdad los organismos solo algoritmos y es en verdad la vida solo procesamiento de datos?; 2. ¿qué es más valioso: la inteligencia o la conciencia?; 3. ¿qué le ocurrirá a la sociedad, a la política y a la vida cotidiana cuando algoritmos no conscientes pero muy inteligentes nos conozcan mejor que nosotros mismos? "*[4]

Esta última pregunta: "*¿qué le ocurrirá a la sociedad, a la política y a la vida cotidiana cuando algoritmos no conscientes pero muy inteligentes nos conozcan mejor que nosotros mismos?"*[5], me resulta de mucho impacto, creo que refleja parte del gran fenómeno que estamos atravesando, que tiene consecuencias en todo y en todos, a gran velocidad y que genera grandes cambios.

No podemos ver al mundo digital como algo diferente al mundo tradicional, sino que debemos contextualizar que ambos conviven, convergen, el mundo es uno. Lo que debemos hacer es recibirlo, buscando el desarrollo sostenible para todos, para lo cual, en línea con lo manifestado por la Naciones Unidas para alcanzar los Objetivos de Desarrollo Sostenible, es fundamental *"la colaboración de los gobiernos, el sector privado, la sociedad civil y los ciudadanos por igual para asegurar que dejaremos un mejor planeta a las generaciones futuras"*[6].

Sin lugar a duda todo este nuevo contexto genera múltiples retos para el Derecho, en tanto busca la justicia, el equilibrio, debiendo necesariamente reflejar la realidad y las necesidades; pero también abre un mundo de oportunidades, siendo cada vez más inminente la revisión de las regulaciones, a fin de responder adecuadamente a las nuevas necesidades socioeconómicas.

---

3 NOAH HARARI, YUVAL, *"Homo Deus - Breve Historia del mañana",* Debate, España. 2016. URL: https://www.beek.io/frases/homo-deus-breve-historia-del-manana Consultado el 10 de diciembre de 2020.

4 NOAH HARARI, YUVAL, Obra citada.

5 NOAH HARARI, YUVAL, Obra citada.

6 NACIONES UNIDAS, Objetivos de Desarrollo Sostenible. URL: http://www.undp.org/content/undp/es/home/sustainable-development-goals.html. Consultado el 20 de enero de 2019.

II. La revolución digital[7]

Estamos ante una nueva revolución, la revolución digital o 4.0, la cual se caracteriza por venir a cambiarlo todo, alcanzando a todos y a todo, a una velocidad impensada.

Como se establece en el Diccionario de la Real Academia Española, por "Revolución" entendemos, entre otras cosas: "*1.f. Acción y efecto de revolver o revolverse", "2.f. Cambio profundo, generalmente violento, en las estructuras políticas y socioeconómicas de una comunidad nacional"*[8]*;* y por "Digital" "*4.adj. Que se realiza o transmite por medios digitales"*, "*5.adj. Dicho de algunos medios de comunicación, especialmente de prensa: que se publican en Internet o en formato electrónico"*[9].

La Cumbre Mundial sobre la Sociedad de la Información define a la Revolución Digital indicando que *"El rápido desarrollo de las tecnologías de la información y las comunicaciones y la innovación de los sistemas digitales representan una revolución, que ha cambiado fundamentalmente la manera en que la gente piensa, actúa, comunica, trabaja y gana su sustento.*[10]*"*

En este sentido, podemos afirmar que la revolución digital viene a cambiar las estructuras políticas y socioeconómicas de las sociedades tal como las conocemos, y lo hace a través de Internet o en formato electrónico[11].

Esta revolución ha sido consecuencia del gran avance que han tenido las redes de telecomunicaciones, la convergencia tecnológica y especialmente de Internet. Lo anterior, sumado al desarrollo de las plataformas electrónicas, han hecho posible que se conecte gran parte de la población –aunque aún faltan muchos por conectar–, que se atiendan diversas necesidades sociales, al tiempo que se generen grandes avances tecnológicos, que potencian aún más la revolución digital, generando cambios económicos y sociales de impacto.

---

7 Véase nuestro trabajo en ARAMENDÍA, MERCEDES, "La Revolución Digital: telecomunicaciones, servicios digitales y la sociedad de la información", *Estudios de Telecomunicaciones y Sociedad de la Información.* Universidad de Montevideo. 2018, pp. 4 y ss.

8 Diccionario de la Real Academia Española, definición de "Revolución": http://dle.rae.es/?id=WQ0Bykx ◇ Consultado el 4 de octubre de 2017.

9 Diccionario de la Real Academia Española, definición de "Digital": http://dle.rae.es/?id=Dl56Lag ◇ Consultado el 4 de octubre de 2017.

10 UIT: https://www.itu.int/net/wsis/basic/faqs_answer.asp?lang=es&faq_id=42 ◇ Consultado el 5 de octubre de 2017.

11 ARAMENDÍA, MERCEDES, obra citada, pp. 5 y ss.

El contexto debe desarrollarse de manera conjunta, en este sentido es importante considerar a todo el "ecosistema digital", a efectos de impulsar los diversos elementos necesarios para que todos podamos ser parte.

Hay múltiples factores a considerar, en anteriores trabajos he destacado principalmente tres[12]: (1) el despliegue de redes de telecomunicaciones; (2) el impulso de la sociedad de la información y del conocimiento, comprendiendo el impulso de diversos servicios y aplicaciones digitales; y (3) el desarrollo de habilidades digitales, destacando la importancia de la educación y de la confianza.

Mas, considero que también hay otros factores muy importantes que son esenciales para el desarrollo de las tecnologías más avanzadas, como es el desarrollo de la capacidad de procesamiento y de almacenamiento de datos.

El despliegue de redes de telecomunicaciones es fundamental para facilitar la conectividad y la digitalización, sobre las mismas se desarrolla la sociedad de la información y del conocimiento, siendo esencial que todas las personas tengan acceso de calidad, para lo cual es imprescindible el trabajo en conjunto de toda la sociedad, públicos, privados, academia y sociedad civil, así como de todos los interesados en aportar.

En el gran desarrollo que han tenido las telecomunicaciones, la convergencia y la Internet juegan un rol esencial, en tanto hacen posible que servicios completamente diferentes sean prestados utilizando la misma red. De esta manera, ahora la prestación de un servicio no necesariamente debe estar relacionado con la provisión de una red. En tanto, la evolución tecnológica y de los mercados ha generado que las redes utilicen la tecnología de Internet (ip), al tiempo que los usuarios sustituyen los servicios tradicionales –como los mensajes de texto (sms) o la telefonía de voz– por servicios equivalentes pero que son prestados sobre la red ip, como por ejemplo voz sobre ip (voip). Al usuario final le es indiferente si el proveedor transporta él mismo la señal o si lo hace a través de un servicio de acceso a Internet.[13]

12 ARAMENDÍA, MERCEDES, obra citada, pp. 6 y ss.

13 Exposición de Motivos Directiva (UE) 2018/1972 del Parlamento Europeo y de Consejo de 11 de diciembre de 2019 por la que se establece el Código Europeo de las Comunicaciones Electrónicas.

Lo anterior muestra el rol fundamental que juega el principio de neutralidad tecnológica, en tanto facilita la innovación y que la evolución siga su curso. Al respecto, como surge de la exposición de motivos del Código de Comunicaciones Electrónicas de la Unión Europea (ue), interesa destacar: (i) que las capacidad de las redes de comunicaciones electrónicas están en constante aumento, (ii) que parámetros como la latencia, la disponibilidad y la fiabilidad toman cada vez mayor importancia, (iii) que el medio a través del cual se presta un servicio de conectividad va a ser cada vez menos importante, en tanto ofrezcan un rendimiento de red similar, (iv) que la neutralidad tecnológica solo debe aplicarse ante la necesidad de evitar interferencias perjudiciales, (v) que no se debería excluir la posibilidad de utilizar más de un servicio en la misma banda de espectro radioeléctrico, sino que los usuarios de mismo deberían poder elegir las tecnologías y los servicios, a menos que estén en juego objetivos de interés general, debidamente justificado y revisados periódicamente[14].

Por otra parte, en relación con el impulso de la sociedad de la información y del conocimiento. Cabe entender por "Sociedad de la Información" aquella que viene determinada *"por la extraordinaria expansión de las redes de telecomunicaciones y, en especial, de Internet como vehículo de transmisión e intercambio de todo tipo de información. Su incorporación a la vida económica y social ofrece innumerables ventajas, como la mejora de la eficiencia empresarial, el incremento de las posibilidades de elección de los usuarios y la aparición de nuevas fuentes de empleo.*[15]*"*

Los diversos servicios y aplicaciones digitales que se desarrollan en la sociedad de la información responden y pretenden atender diversas necesidades sociales y económicas; y junto con las tecnologías avanzadas, ofrecen innumerables ventajas, al tiempo que permiten crear nuevos modelos económicos, desarrollar ciudades, casas, autos y múltiples cosas inteligentes. Asimismo, al incluir la tecnología en áreas tradicionales, generan grandes cambios y retos, como puede ser en el Derecho (Legaltech), en las finanzas (Fintech), en los seguros (Insurtech), en la regulación (Regtech), entre otros múltiples ejemplos.

Ante estos grandes cambios, la integración es esencial, para lo cual se debe trabajar en desarrollar las habilidades digitales de todas las personas, destacando la

14 Código Europeo de las Comunicaciones Electrónicas.

15 Exposición de motivos de la Ley N° 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico.

importancia de la educación y de la confianza. Es esencial disminuir la brecha digital, buscando que todas las personas sean parte de esta nueva realidad digital y que sean conscientes de sus implicancias, que puedan utilizar las redes, así como los servicios y aplicaciones digitales que se generan de manera responsable, y así puedan apalancarse en el mundo de oportunidades que la digitalización ofrece.

Junto con este gran desarrollo, las personas compartimos cada vez más datos, los cuales adecuadamente almacenados, procesados y analizados permiten obtener mucha información, de gran valor, en tanto nos permite conocer, prever, así como tomar decisiones más informadas, entre otras utilidades. Mas la cantidad de datos que se generan es inmensa y cada vez se multiplica más. En este sentido, se presenta como fundamental tener las capacidades necesarias para procesarla y tratarla debidamente, así como para poder almacenarla, atendiendo la seguridad desde el diseño y de forma proactiva.

Asimismo, considerando que compartimos cada vez más datos, es primordial empoderar a los ciudadanos, proteger su privacidad, así como sus derechos fundamentales, al tiempo que darles la opción de elegir compartir o no sus datos, sin ser discriminados.

Considerando lo anterior, vale subrayar que puede haber redes de telecomunicaciones muy buenas, así como servicios y aplicaciones digitales extraordinarias, mas si la población no tiene las habilidades, no tiene el conocimiento ni la confianza como para utilizarlas debidamente, tanto las redes como los servicios pierden sentido.

En lo que respecta a la capacidad de procesamiento y de almacenamiento, a fin de mostrar la importancia de estos elementos, es interesante comentar que una de las grandes diferencias entre Deep Blue que en 1996 no derrotó a Gary Kaspárov, campeón del mundo de ajedrez en ese momento, y Deeper Blue, quien en 1997 sí derrotó a Gary Kaspárov; fue justamente la capacidad de procesamiento que le permitía calcular muchas más posiciones, a gran velocidad.[16]

16 Digital Transformation. Curso Online brindado por BCG y University of Virginia a través de Coursera.

Asimismo, interesa subrayar que Boston Consulting Group (bcg)[17], hace énfasis en que la tecnología ha evolucionado de forma exponencial en las últimas décadas y parte de la explicación la basan en tres reglas fundamentales relacionados con la gestión de la información digital. La primer regla es la "Ley de Moore", la cual indica que cada 18 meses cada ordenador duplicará la capacidad para procesar información; la segunda regla es la "Ley de Butters", la cual destaca que la cantidad de información transmitida por una única fibra óptica se duplica cada nueve meses; y la tercer regla, es la "Ley de Kryder", la cual señala que la cantidad de datos almacenados por centímetro cuadrado de una unidad de disco duro se dobla cada 13 meses, en la realidad la tendencia ha disminuido, y se duplica cada 16 o 17 meses. Estas capacidades mejoran el rendimiento de los dispositivos de mercado masivo, al tiempo que reducen los costos para los consumidores, de esta manera no solo son cada vez mejores, sino que además más asequibles[18], lo cual facilita la universalización de estos.

Todos los factores mencionados cumplen un rol esencial para que la transformación digital pueda desarrollarse con éxito. La digitalización facilita y agiliza los procesos, generando múltiples oportunidades, mas requiere de diversas acciones, al tiempo que presenta múltiples desafíos, los cuales debemos identificar a fin de trabajar sobre los mismos, y atender los impactos sociales y económicos que esta nueva realidad genera.

III. La digitalización y el Derecho

Cabe comenzar preguntándonos qué es la digitalización. Si acudimos al Diccionario de la Real Academia Española, la "digitalización" se define como la acción y el efecto de digitalizar[19]. A su vez, "digitalizar" se define como "*1. Registrar datos en forma digital. 2. Convertir o codificar en números dígitos datos o informaciones de carácter continuo, como una imagen fotográfica, un documento o un libro"*[20]. Siguiendo la línea, "*digital"* se define como un dispositivo o un sistema que crea, presenta, transporta o almacena información mediante la combinación de bits[21],

17 Ibídem.
18 Ibídem.
19 Diccionario de la Real Academia Española, definición de "Digitalización". URL: http://dle.rae.es/?id=Dl5l0Y6. Consultado el 15 de enero de 2019.
20 Diccionario de la Real Academia Española, definición de "Digitalizar". URL: http://dle.rae.es/?id=DlBB81T. Consultado el 15 de enero de 2019.
21 Diccionario de la Real Academia Española, definición de "Digital". URL: http://dle.rae.es/?id=Dl56Lag ◇ Consultado el 15 de enero de 2019.

asimismo, suele utilizarse como un sinónimo de "online", "en línea", "conectado", "en Internet" o "electrónico".[22]

Por otra parte, "bit" es un código binario, que emplea solo dos números: el uno (1) o el cero (0), siendo "*una unidad de medida de información* "[23], que, al ser transmitidos por medio de Internet como datos, permiten a los proveedores de servicios y desarrolladores de productos, innovar y desarrollar nuevas opciones a velocidades mucho mayores en comparación a lo que se podía hacer en la forma tradicional.

En esta línea, como señala Raúl Katz: *"La digitalización se refiere a las transformaciones provocadas por la adopción masiva de tecnologías digitales que generan, procesan, comparten y transfieren información. La transformación digital no es un evento de una sola vez. Procede en oleadas impulsadas por el progreso tecnológico y la difusión de innovaciones.*[24]"

Al respecto identifica tres olas. La primera, relacionada con lo que se consideran "tecnologías maduras", como pueden ser las tecnologías de telecomunicaciones (por ejemplo: banda ancha, telecomunicaciones de voz) que permiten el acceso remoto a la información. La segunda, vinculada con la difusión de Internet y sus plataformas (por ejemplo: motores de búsqueda, mercados, etc.) que permiten la conexión en red entre empresas (B2B), entre empresas y consumidores (B2C) y entre consumidores (C2C). La tercera, implica la adopción de tecnologías de avanzada (por ejemplo: *Big data*, Internet de las Cosas, Robótica, Inteligencia Artificial) que permite mejorar el procesamiento de la información y la calidad de la toma de decisiones, así como automatizar tareas rutinarias en empresas y gobiernos.[25]

La digitalización ha sido progresiva, y se ha instaurado como consecuencia del proceso de integración, de adopción y de universalización de estas olas. Cada una, por sí, ha generado impacto en la sociedad, pero las tres actuando conjuntamente es lo que

22 Fundéu BBVA, recomendaciones tras búsqueda "digital". URL: https://www.fundeu.es/recomendacion/online-conectado-digital-electronico-o-en-linea-1416/ Consultado el 15 de enero de 2019.
23 Definición de "Bit", Diccionario de la Real Academia Española. URL: http://dle.rae.es/?id=5cPrUzM Consultado el 15 de enero de 2019.
24 KATZ, RAÚL, *"Social and Economic Impact of Digital Transformation on the Economy"*, informe preparado bajo la dirección de la Unión Internacional de Telecomunicaciones, División de Regulación y Ambiente de Mercado.
25 KATZ, RAÚL, obra citada.

vino a cambiar las estructuras políticas y socioeconómicas de las sociedades tal como las conocemos.

Considerando este escenario, principalmente los impactos que genera, debemos destacar que el Derecho viene a responder y a atender las realidades económicas y sociales, buscando la justicia y el equilibro. Se relaciona con el camino "correcto" que se considera que debe seguir la sociedad en cada momento histórico, lo cual vemos reflejado en el propio término: Retch (alemán), Right (inglés), Droit (francés), Dereito (portugués), Diritto (italiano)[26].

En línea con el contexto, también es importante considerar la tradición y la realidad de cada nación. "Tradición es más que una simple continuidad histórica. Es una mezcla de elementos conscientes e inconscientes*, una suerte de amalgama del "lado más visible de la sociedad –instituciones, monumentos y obras, entre otras cosas– y el lado sumergido e invisible, formado por creencias, deseos, temores, represiones y sueños (…) El Derecho suele asociarse con el lado invisible de la sociedad y sus obras; pero un estudio de la historia del Derecho occidental, y especialmente de sus orígenes, revela su arraigo en las creencias y emociones más profundas de un pueblo (…) Así las cosas, no nos sorprende que cada vez que una sociedad se encuentra en crisis, vuelva instintivamente la mirada a sus orígenes y busque en ellos un signo (…)*[27].

"*Precisamente uno de los cambios más significativos en la historia del Derecho romano vendrá de la mano del reconocimiento jurídico de la voluntad del sujeto de derecho como instrumento operativo en el mundo de los negocios. Una voluntad libremente manifestada con cualesquiera palabras inteligibles y expresivas del consentimiento. Una voluntad capaz de crear vínculos entre quienes consienten, y una voluntad capaz de conformar la posición jurídica de quienes manifiestan sus disposiciones. (…). Las palabras son ahora expresivas de la voluntad ciertamente querida por el sujeto de derecho que se manifiesta en un determinado sentido. El rito, la liturgia y la ceremonia como moldes formales de creación de derechos y obligaciones han perdido en buena medida su valor constituyente. La nueva historia de la experiencia jurídica romana gravita alrededor del derecho señalado por el*

26 CASTRESANA, AMELIA, *Derecho Romano. El arte de lo bueno y de lo justo.* Tercera Edición. Tecnos. Año2017. p. 95.

27 "Son palabras de Octavio PAZ citadas por H .J. BERMAN, La formación de la tradición jurídica de Occidente, trad. M. ULTRILLA DE NEIRA, México, 1996, p. 586; citado a su vez por CASTRESANA, AMELIA en *Derecho Romano.* Obra citada, p. 12.

magistrado y de las soluciones de justicia propuestas por los juris consultores: el Derecho se transforma en justicia, en el arte de lo bueno y de lo justo."[28]

El Derecho para poder ser efectivamente el arte de lo bueno y de lo justo, necesariamente debe aggionarse a la realidad, a la sociedad, a las instituciones, teniendo en cuenta las bases, los pilares y los principios que rigen. A lo largo de la historia, necesariamente las normas se han tenido que actualizar, modernizar, ponerse al día para poder reflejar la realidad y las necesidades de la sociedad. Para ello no necesariamente se tiene que regular, sino que se tiene que hacer un análisis cabal, debiendo en algunos casos desregular y en otros actualizar.

En muchos casos, se ha procurado responder a esta nueva realidad, regulando y pretendiendo que la misma encaje en normativas pensadas para supuestos completamente diferentes.

Considero que el punto de partida debe ser diferente y que debemos empezar por reconocer, entre otras cosas, los siguientes aspectos[29]:

i. Que la digitalización impacta a todos y en todo a velocidades exponenciales, lo cual no nos permite responder a tiempo ni de la forma más adecuada –y procurar hacerlo podría ser peligroso, en tanto se podría afectar la innovación sin siquiera advertirlo–, lo cual hace que los principios generales tomen cada vez mayor importancia.

ii. Que el derecho siempre fue pensado para una realidad física, tangible, diferente a la actual, e incluso si se protegían intangibles como ser la propiedad intelectual, en general estaban sobre un tangible, como ser un libro o un disco.

iii. Que la información es un producto, es valor, y es muy difícil de proteger porque es fácilmente escalable, replicable y transmisible.

iv. Que un acercamiento fragmentado, como siempre se hizo en el Derecho, ya no resulta suficiente, siendo cada vez más necesario atender soluciones universales y flexibles. Internet no conoce fronteras.

---

28 Citado por CASTRESANA, AMELIA en obra citada, p. 14, "Textos de cabecera del Digesto de Justiniano transcriptos por A. FERNÁNDEZ DE BUJÁN en su artículo de opinión "Actualidad del Derecho Romano", en el diario ABC, 29 de abril de 2015.

29 MURRAY, ANDREW, *"Information Technology Law. The Law and Society*", pp. 12 y ss. Third edition. Oxford, 2016.

v. Que la digitalización se hace sobre Internet, lo cual se reconoce como *"…el sistema adaptativo complejo más grande y de más rápida evolución en la Historia de la Humanidad"*[30], *y* que ha cambiado drásticamente en los últimos años, principalmente por cuatro grandes cambios[31]: (1) Por el gran aumento en el número y en el tipo de usuarios. Cuando comenzó Internet se utilizaba por pequeños grupos de científicos e investigadores, hoy el uso es universal y constante, cada vez hay más personas y objetos que se conectan a la red. (2) Por la gran variedad y cantidad de aplicaciones. Los usos son cada vez más variados: correo electrónico, buscador, juegos, videoconferencias, almacenamiento, etc. (3) Por el desarrollo de nuevas tecnologías con más cobertura, capacidad y velocidad, simplifican el uso y la universalización. Son fundamentales para responder al uso masivo, así como desarrollar nuevos servicios y aplicaciones digitales. (4) Por el desarrollo de relaciones de negocio más complejas. *"A mediados de los años noventa, la topología de Internet se basaba en una estricta jerarquía de tres niveles: troncales, proveedores de servicios de Internet de áreas o regiones, y proveedores que daban servicio en la llamada "última milla". Ahora, Internet se caracteriza por un conjunto mucho más diverso de relaciones comerciales como, por ejemplo, el "el peering" entre particulares o las redes de distribución de contenidos."*[32]

Vale mencionar además que, en este nuevo mundo, las barreras de entrada en los diversos mercados suelen diluirse, las rivalidades ya no son necesariamente entre otros prestadores que realizan las mismas actividades (por ejemplo: entre operadores de servicios de telecomunicaciones o entre bancos), sino que la competencia se amplía. Nuevos proveedores de servicios, especializados, pueden competir en determinados segmentos con los negocios tradicionales y, en muchos casos, estos servicios específicos, que compiten con los tradicionales, utilizan la infraestructura de los operadores tradicionales. A modo de ejemplo: (i) Whatsapp utiliza la red de los operadores de telecomunicaciones para prestar sus servicios, con quienes a su vez compite en los sms y en las llamadas de voz; (ii) PayPal utiliza en algunos casos las

30 GARCÍA MEXÍA, PABLO, J. D., "*El derecho de Internet"* - Francisco PÉREZ BES (Coordinador), Atelier Libros Jurídicos. Capítulo I, p. 17, citando al Consejo para la Agenda Global del Foro de Davos (GAC en inglés).

31 GARCÍA MEXÍA, PABLO, J.D.: en obra citada, p. 17.

32 GARCÍA MEXÍA, PABLO, J.D.: en obra citada, p. 17.

cuentas bancarias de los usuarios, compitiendo con los bancos en el segmento de pagos *online*[33].

Todos estos cambios presentan desafíos políticos, económicos y sociales. Tanto las personas físicas, como la sociedad civil, las empresas y los gobiernos necesariamente deben *aggionarse* para poder responder adecuadamente a los nuevos retos que el mundo digital conlleva.

En esta línea, reconociendo la importancia y los desafíos que el mundo digital detenta, tanto a nivel regional como nacional; gobiernos y organizaciones están trabajando en agendas digitales, a fin de poder prepararse y crear las condiciones para que esta nueva realidad pueda desarrollarse de la mejor manera.

El centro de todo siempre tiene que ser las personas y tenemos que trabajar para garantizar que sus derechos fundamentales sean respetados, así como para que se revean las reglas de juego que se aplican, buscando disponer las mismas reglas para los mismos servicios, independientemente del medio a través del cual se brindan.

IV. Agendas digitales

En vista de la gran evolución que ha tenido el mundo digital, tanto a nivel regional como a nivel país, se han desarrollado diversas agendas digitales.

Por ejemplo, a nivel regional, la Unión Europea ya en el año 2010 aprobó la Agenda Digital para impulsar la economía, aprovechando las ventajas económicas y sociales del mercado único digital[34]. Asimismo, en América Latina y el Caribe, desde el año 2003 en el marco de la Cumbre Mundial sobre la Sociedad de la Información, con la colaboración de cepal, se está trabajando en un Plan de Acción sobre la Sociedad de la Información (eLAC2007, eLAC2015), en el 2015 aprobaron la Agenda Digital para América Latina y el Caribe (eLAC2018) y en el 2018 la Agenda Digital eLAC2020. A nivel Mercosur también se está trabajando en la temática.

A nivel país, Uruguay ya ha aprobado cuatro agendas digitales, en base a las cuales desarrolla diversos proyectos y líneas de acción, y España no solo cuenta con su

33 Digital Transformation, curso online citado.

34 Agenda Digital para Europa. URL: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&ved=2ahUKEwiXp_aZ9obgAhWFZd8KHf73BLMQFjABegQICBAC&url=https %3A %2F %2Feuropa.eu %2Feuropean-union %2Ffile %2F1501 %2Fdownload_es %3Ftoken %3D3l7D0Fil&usg=AOvVaw2MfLhfsJnPmv5J3AOt6TJ_ . Consultado el 15 de enero de 2019.

Agenda Digital desde larga data, sino que además dispone de un Ministerio específico que atiende la temática.

Si bien procedemos a comentar las agendas mencionadas, vale destacar que hay diversos niveles de avance y que hay factores comunes en todas las agendas, como son: el despliegue de redes de última generación, el conectar a todos, el generar más servicios y aplicaciones digitales, extender las competencias y habilidades digitales de las personas, desarrollar la economía digital y proteger los derechos humanos fundamentales.

(IV.1). Agenda Digital Unión Europea (UE)

En comunicación titulada "Europa 2020 - Una estrategia para el crecimiento inteligente, sostenible e integrador" (com [2010] 2020)[35], la Comisión Europea presentó diversas iniciativas para potenciar la economía, entre ellas la Agenda Digital, partiendo de la base de que la economía digital crece siete veces más deprisa que el resto de la economía, pero que la fragmentación del marco político afecta su potencial. Reconocen que hay millones de personas que aún no utilizan Internet, que hay quienes tienen más dificultades, que cada vez se necesita más Internet para las tareas diarias, requiriendo mayor capacidad digital y mayores competencias en tecnologías de la información y las comunicaciones.[36]

Entre los retos, parten de la base de que de la banda ancha es oxígeno para todos, que el desarrollo de redes de alta velocidad tiene el mismo impacto que en el siglo pasado tuvieron las redes eléctricas y de transporte, para lo cual busca su expansión a través de la reducción de costes, recomendaciones sobre redes de próxima generación, revisión de directrices sobre ayudas estatales a la banda ancha, completar el mercado único de las telecomunicaciones y conseguir un continente conectado.

De esta manera entienden que habrá más economía de escala, más innovación, más diversificación de productos y de servicios.

Entre los principales elementos para alcanzar lo anterior, destacan la necesidad de una Internet abierta, que se refuercen los derechos de los consumidores, que se eliminen

35 Parlamento Europeo. URL: http://www.europarl.europa.eu/factsheets/es/sheet/43/el-mercado-unico-digital-omnipresente ◇ Consultado el 15 de enero de 2019.
36 Agenda Digital para Europa, obra citada.

las tarifas extras, que se coordine la asignación de espectro radioeléctrico y que haya seguridad jurídica para los inversores.

Se busca reforzar el entorno empresarial de las tecnologías web y de la información, ayudando a los emprendedores a encontrar recursos, facilitando el comercio electrónico, que los consumidores puedan acceder a las tiendas *online*, al tiempo que las empresas puedan ofrecer sus servicios en otros países.

Para esto se dispone objetivos relacionados con mejorar la entrega por correo postal, facilitar el pago electrónico, móvil o con tarjetas, estimulando la confianza, para lo cual se debe dar seguridad y protección.

Se reconoce que gran parte de la población no tiene los conocimientos digitales suficientes para el entorno laboral actual, lo cual va en clara contraposición con la demanda y las necesidades de las empresas, que cada vez más requieren especialistas en tecnología de la información y las comunicaciones.

En 2015 la Comisión Europea señaló[37] que la estrategia para el mercado único digital se basaba principalmente en tres pilares: (1) mejorar el acceso de los consumidores y de las empresas a los bienes y servicios digitales, (2) crear las condiciones y garantizar la igualdad de condiciones para que las redes digitales y los servicios innovadores pudieran prosperar, y (3) maximizar el potencial de crecimiento de la economía digital.

Con relación al primer pilar, para mejorar el acceso de los consumidores y de las empresas a los bienes y servicios digitales, se dispuso, entre otras acciones, las siguientes:

i. Dictar normas para facilitar el comercio electrónico transfronterizo. Por ejemplo: armonizar contratos, proteger a los consumidores, facilitar que las empresas puedan vender.

ii. Paquetería más eficiente y asequible.

iii. Determinar problemas de competencia que afecten a los mercados.

37 Comisión Europea, Comunicado de prensa. URL: http://europa.eu/rapid/press-release_ip-15-4919_es.htm Consultado el 15 de enero de 2019.

iv. Actualizar los derechos de autor, mejorando el acceso de los ciudadanos a los contenidos culturales en línea, ofreciendo a su vez nuevas oportunidades a los creadores y a la industria de contenidos.

v. Reducir las cargas administrativas consecuencia de diferentes regímenes.

Respecto al segundo pilar, para crear las condiciones adecuadas y garantizar la igualdad de condiciones para que las redes digitales y los servicios innovadores puedan prosperar, la Comisión dispuso, entre otras acciones, las siguientes:

i. Revisar la normativa sobre telecomunicaciones, lo cual implica coordinar la asignación del espectro, crear incentivos a la inversión en banda ancha de alta velocidad, garantizar la igualdad de condiciones para todos los agentes del mercado, y crear un marco institucional eficaz.

ii. Revisar el marco de comunicación audiovisual con el fin de adecuarlo al siglo XXI, centrándose en las funciones de los distintos agentes del mercado en la promoción de las obras europeas, analizando su adopción a los nuevos modelos empresariales para la distribución de contenidos.

iii. Analizar el papel de las plataformas en línea (motores de búsqueda, redes sociales, tiendas de aplicaciones, etc.) en el mercado, abarcando cuestiones como la transparencia de los resultados de la búsqueda y de las políticas de fijación de precios, el uso de la información obtenida, las relaciones entre plataformas y proveedores.

iv. Reforzar la confianza y la seguridad en los servicios digitales, en particular en relación con el tratamiento de datos personales.

v. Buscar seguridad en línea.

Finalmente, sobre el tercer pilar, para maximizar el potencial de crecimiento de la economía digital, entre otras iniciativas, se dispuso:

i. Proponer una regulación de libre flujo de datos no personales y otra sobre computación en la nube.

ii. Definir normas e interoperabilidad.

iii. Apoyar una sociedad integradora en la que los ciudadanos tengan las cualificaciones adecuadas para aprovechar las oportunidades, y un plan de acción para la administración electrónica que conecte los registros mercantiles en toda Europa.

En 2016 la Comisión Europea destacó que *"Tenemos que estar conectados. Nuestra economía lo necesita. La gente lo necesita. Y tenemos que invertir en esa conectividad ahora mismo"*. En consecuencia, dispuso tres objetivos estratégicos de conectividad para 2025: (1º) todos los motores socioeconómicos relevantes[38] tienen que acceder a una conectividad alta, como mínimo que permita descargas y/o cargas de 1 Gigabit de datos por segundo; (2º) todos los hogares tengan acceso a una conectividad que como mínimo ofrezca una velocidad de descarga de 100 Mbps; y (3º) todas las zonas urbanas, las principales carreteras y ferrocarriles, tienen que tener cobertura ininterrumpida del sistema de comunicación 5G, el cual debe estar al 2020 al menos en una de las principales ciudades de cada Estado miembro. Se reconoce que para alcanzar estos objetivos se necesitan grandes inversiones, por lo cual se aprobó un nuevo Código Europeo de las Comunicaciones Electrónicas, que contiene normas orientadas al futuro, a fin de hacer más atractiva la inversión[39].

En el año 2017, la Comisión Europea[40] realizó un balance de los progresos alcanzados y presentó el camino por recorrer en tres ámbitos fundamentales:

1. La economía de los datos: destaca que se está trabajando en una iniciativa para la libre circulación de datos no personales dentro de la Unión Europea –dicha normativa fue aprobada en octubre de 2018[41]–, y hace referencia a una iniciativa sobre accesibilidad y reutilización de los datos públicos y receptores de financiación pública –se realizó una consulta pública en el año 2018 para revisar la Directiva relativa a la reutilización de la información del sector público[42]–.

2. La ciberseguridad: señala que se revisaría la estrategia y el mandato de la Agencia Europea de Seguridad de las Redes y de la Información (enisa). En mayo de 2018 se aprobó la Directiva sobre seguridad de las redes y sistemas de información

---

[38] Como ser: los centros educativos, de investigación, nudos de transporte, los proveedores de servicios públicos, como los hospitales y las administraciones públicas, así como las sociedades o empresas que necesiten de las tecnologías digitales.

[39] Comisión Europea. URL: https://ec.europa.eu/commission/presscorner/detail/es/IP_16_3008 Consultado el 1º de junio de 2019.

40 Comisión Europea, Comunicado de Prensa. URL: http://europa.eu/rapid/press-release_ip-17-1232_es.htm Consultado el 15 de enero de 2019.

41 Reglamento relativo a un marco para la libre circulación de datos no personales en la UE. URL: http://data.consilium.europa.eu/doc/document/pe-53-2018-init/en/pdf Consultado el 15 de enero de 2019.

42 Consulta Pública relativa a la reutilización de la información del sector público. URL: https://ec.europa.eu/info/consultations/public-consultation-review-directive-re-use-public-sector-information-psi-directive_es Consultado el 15 de enero de 2019.

(Directiva sri)[43]. El 24 de enero de 2019 se publicaron buenas prácticas para la implementación de estándares técnicos regulatorios[44].

3. Plataformas en línea: busca abordar las cuestiones vinculadas con las cláusulas contractuales abusivas y las prácticas comerciales desleales. Vale señalar que en abril de 2018 establecieron nuevas normas que buscan aumentar la transparencia y resolver con más eficacia los litigios[45].

En esta línea, la Comisión Europea destaca que el mercado único digital busca un mercado único de bienes y servicios en todo su territorio, mediante la eliminación de las barreras reglamentarias que obstaculicen el uso de servicios y tecnologías digitales en línea. Ha sido identificado como una de sus diez prioridades, en tanto mejora el acceso a la información y a la cultura, incrementa las oportunidades de empleo, promueve una forma de gobierno moderna y abierta, siendo fundamental para la economía de Europa[46].

En el 2018 la Comisión Europea publicó los resultados del índice de la Economía y la Sociedad Digital (desi)[47], destacan entre otras cosas: (i) que la conectividad ha mejorado, pero que es insuficiente frente a la necesidad; (ii) que se está trabajando en una reforma de las normas de la UE sobre telecomunicaciones para atender la creciente demanda y potenciar las inversiones; (iii) que cada vez más europeos utilizan Internet para comunicarse; (iv) que hay más especialistas que antes, pero aún no los suficientes; (v) que las empresas se digitalizan y el comercio electrónico se desarrolla de manera lenta; y (vi) que se utilizan más los servicios públicos en línea.

---

43 Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo de 6 de julio de 2016 relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión.

44 ENISA, Good practices in the implementation of regulatory technical standards. URL: https://www.enisa.europa.eu/news/enisa-news/good-practices-in-the-implementation-of-regulatory-technical-standards Consultado el 15 de enero de 2019.

45 Comisión Europea. Plataformas en línea. URL: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A52016DC0288 Consultado el 15 de enero de 2019.

46 Comisión Europea, el Mercado Único Digital. URL: http://publications.europa.eu/webpub/com/factsheets/digital/es/#what-is-digital-single-market Consultado el 15 de enero de 2019.

47 Comisión Europea, Comunicado de prensa. URL: http://europa.eu/rapid/press-release_ip-18-3742_es.htm Consultado el 15 de enero de 2019.

Para seguir profundizando el mercado único digital fiable: (i) se aprobó el Reglamento General de Protección de Datos[48]; (ii) se propuso el Reglamento sobre el respeto de la vida privada y la protección de los datos personales en el sector de las comunicaciones electrónicas y por el que se deroga la Directiva 2002/58/CE (Reglamento sobre la privacidad y las comunicaciones electrónicas)[49]; (iii) se aprobó el Reglamento sobre la libre circulación de datos no personales[50]; (iv) se aprobó el Código de las Comunicaciones Electrónicas[51]; (v) se invita a movilizar inversiones públicas y privadas necesarias para desplegar la inteligencia artificial, las redes de conectividad 5G y de alto rendimiento; y (vi) se destaca la importancia de ayudar a dotar a las personas con las competencias digitales que necesitarán para la economía y la sociedad digital.

En definitiva, como surge de lo expuesto, desde el año 2010 se han llevado múltiples acciones a fin de hacer efectivo el Mercado Único Digital. Es fundamental trabajar en todo el ecosistema, de manera de poder hacer realidad y universal los objetivos buscados.

(IV.2.) Agenda Digital para América Latina y El Caribe (eLAC 2020) [52]

Como antecedente se destaca la Agenda 2030 para el Desarrollo Sostenible aprobada por la Asamblea General de las Naciones Unidas en setiembre de 2015, donde se establecen 17 objetivos y 169 metas. Asimismo, se tiene en cuenta que en diciembre de 2015, la Asamblea General –al realizar el examen general de la aplicación de los resultados de la Cumbre Mundial sobre la Sociedad de la Información, reafirmando los compromisos con la Declaración de Principios de Ginebra, el Plan de Acción de Ginebra, el Compromiso de Túnez y la Agenda de Túnez para la Sociedad de la

48 Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo , de 27 de abril de 2016, 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 (Reglamento general de protección de datos).

49 Propuesta de Reglamento sobre el respeto de la vida privada y la protección de los datos personales en el sector de las comunicaciones electrónicas. URL: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A52017PC0010 Consultado el 15 de enero de 2019.

50 Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a un marco para la libre circulación de datos no personales en la Unión Europea. URL: https://eur-lex.europa.eu/legal-content/es/txt/?uri=celex:52017pc0495 Consultado el 15 de enero de 2019.

51 Directiva (UE) 2018/1972 del Parlamento Europeo y del Consejo, de 11 de diciembre de 2018, por la que se establece el Código de las Comunicaciones Electrónicas.

52 Agenda Digital para América Latina y el Caribe (eLAC2020). URL: https://conferenciaelac.cepal.org/6/sites/elac2020/files/cmsi.6_agenda_digital.pdf Consultado el 15 de enero de 2019.

Información– reafirmó la necesidad de que los diversos actores - gobiernos, sector privado, sociedad civil, organizaciones internacionales, comunidad técnica y académica, así como todos los demás interesados– trabajen en conjunto para aplicar la visión de la Cumbre Mundial sobre la Sociedad de la Información, después del 2015.

En vista de lo anterior, se aprobó en 2005 el Plan de Acción sobre la Sociedad de la Información eLAC2007, en 2008 el Plan de Acción eLAC2010, en 2010 el Plan de Acción eLAC2015, en 2013 el Plan de Trabajo 2013-2015 para la Implementación del Plan de Acción sobre la Sociedad de la Información y del Conocimiento para América Latina y el Caribe, en 2015 la Agenda Digital para América Latina y el Caribe eLAC2018, y finalmente en 2018 eLAC2020.

Esta última agenda, se aprobó en abril de 2018 durante la Sexta Conferencia Ministerial sobre la Sociedad de la Información en América Latina y el Caribe, con el objetivo de coordinar la cooperación regional en materia digital. Incluye siete áreas de acción y treinta objetivos.

Las áreas de acción son las siguientes: (1) Infraestructura digital; (2) Transformación digital y economía digital; (3) Mercado digital regional; (4) Gobierno digital; (5) Cultura, inclusión y habilidades digitales; (6) Tecnologías emergentes para el desarrollo sostenible; y (7) Gobernanza para la sociedad de la información.

A continuación, se proceden a mencionar los objetivos que integran cada línea de acción, en tanto permiten comprender el alcance y los fines buscados.

Sobre la primera línea de acción, infraestructura digital. El objetivo 1 se enfoca en promover acciones como las siguientes: (i) elaborar e implementar planes de banda ancha con metas concretas y medibles para el despliegue de redes de alta capacidad, (ii) gestionar eficientemente el espectro radioeléctrico, buscar la masificación en el acceso a los servicios de comunicación, (iii) impulsar la inversión para la prestación de los servicios en condiciones asequibles y de calidad, especialmente en zonas remotas, desatendidas, como pueden ser las áreas rurales. El objetivo 2 busca impulsar e incentivar el despliegue de infraestructura y de las tecnologías para el desarrollo de Internet. El objetivo 3 dispone promover el uso de protocolos y de tecnologías resiliente que den soporte, prevengan, mitiguen y permitan la rápida recuperación ante desastres naturales.

Sobre la segunda línea de acción, transformación y economía digital. El objetivo 4 prevé impulsar el uso de tecnologías digitales en las empresas y promover la transformación digital. El objetivo 5 dispone que se estimule el emprendimiento, la innovación basada en datos y que se aceleren los emprendimientos con base tecnológica. El objetivo 6 busca facilitar el desarrollo de fondos de capital de riesgo, tradicionales y no tradicionales, para ofrecer recursos. El objetivo 7 señala que se promueva el teletrabajo y el desarrollo de habilidades digitales.

Sobre la tercera línea de acción, el mercado digital regional. El objetivo 8 dispone que se incremente el comercio y la economía digital, que se fortalezca la competitividad, que se desarrollen plataformas digitales de bienes, servicios y contenidos, y que se promueva el flujo transfronterizo de datos. El objetivo 9 señala que se facilite el comercio regional, a través del uso de tecnologías, de la coordinación institucional y la interoperabilidad de los diferentes sistemas nacionales de comercio exterior.

Sobre la cuarta línea de acción, el gobierno digital. El objetivo 10 busca impulsar estándares de servicios digitales que faciliten y agilicen los servicios gubernamentales y promuevan múltiples canales de acceso. El objetivo 11 señala que se promueva el uso de componentes reutilizables y soluciones abiertas. El objetivo 12 dispone que se adopte una estrategia regional de estándares para la gestión e interoperabilidad de la identidad digital, la firma digital o electrónica avanzada, la apostilla electrónica y la historia clínica electrónica, preservando la privacidad de la información, fortaleciendo la seguridad y la confianza en las transacciones en línea. El objetivo 13, busca facilitar la apertura y la reutilización de datos, la colaboración, la participación ciudadana, la innovación social, la transparencia pública y la rendición de cuentas. El objetivo 14 promueve el uso de sistemas digitales para compras gubernamentales, contrataciones de servicios y obras públicas, que permita asegurar la transparencia, la vigilancia ciudadana y una efectiva rendición de cuentas.

Sobre la quinta línea de acción, la cultura, la inclusión y las habilidades digitales. El objetivo 15 impulsa el desarrollo y la incorporación de habilidades digitales y de pensamiento computacional en los procesos de enseñanza y aprendizaje, mediante la actualización de los contenidos curriculares, acorde a las capacidades que demandarán las actividades del futuro. El objetivo 16 promueve el fortalecimiento de las habilidades digitales avanzadas, técnicas y profesionales, además de proveer incentivos para que las

empresas y los gobiernos capaciten continuamente a sus trabajadores y se mejore la productividad y la eficiencia. El objetivo 17 busca promover la producción, oferta y uso de los contenidos, bienes y servicios digitales como condición necesaria para la inclusión de personas con discapacidad y personas mayores en la sociedad de la información, especialmente para el trabajo, la educación, el acceso a la justicia, los servicios públicos y las ciudades inteligentes. El objetivo 18 quiere masificar el acceso a servicios digitales y la producción y oferta de contenidos, asegurando la inclusión de toda la población, estimulando también la producción, la oferta y el uso de contenidos en lenguas indígenas y originarias. El objetivo 19 dispone promover una cultura digital, que incentive en los habitantes el desarrollo de habilidades y competencias digitales para el uso innovador, seguro y responsable de las TIC para una convivencia pacífica en línea.

Sobre la sexta línea de acción, tecnologías emergentes para el desarrollo sostenible. El objetivo 20 prevé promover el diseño de políticas públicas apoyadas en la innovación basada en datos y alineadas con las prioridades y estrategias nacionales y regionales. El objetivo 21 dispone impulsar en los procesos de formulación e implementación de las políticas públicas y diseño de servicios digitales, el uso convergente de diferentes tipos de tecnologías emergentes. El objetivo 22 establece promover servicios financieros digitales como una prioridad para desarrollar sistemas financieros inclusivos, mediante la innovación, un marco regulatorio habilitante, el fortalecimiento de habilidades digitales, la gestión financiera responsable, la seguridad y el fortalecimiento de los sistemas de identificación.

Sobre la séptima línea de acción, gobernanza para la sociedad de la información. El objetivo 23 dispone promover una perspectiva integral de igualdad de género en las políticas públicas de desarrollo digital, asegurando el pleno acceso y uso de las TIC a las mujeres y niñas, además del impulso de su participación y liderazgo en espacios públicos y privados de decisión. El objetivo 24 señala prevenir y combatir el cibercrimenes mediante políticas públicas y estrategias de seguridad digital, el desarrollo y/o establecimiento de marcos normativos, el fortalecimiento de capacidades y la coordinación local, regional e internacional entre equipos de respuesta a incidentes informáticos. El objetivo 25 prevé promover la participación de los países de América Latina y el Caribe en los procesos de gobernanza de Internet, reforzando los mecanismos regionales, fortaleciendo capacidades, promoviendo sinergias, fomentando

el desarrollo de espacios de diálogo y mecanismos nacionales de múltiples partes interesadas. El objetivo 26 destaca fortalecer la institucionalidad de las entidades responsables de diseñar, implementar, dar seguimiento y continuidad a las políticas públicas de transformación y las agendas digitales nacionales, y promover la articulación y participación de las distintas partes interesadas en el desarrollo de estas políticas. El objetivo 27 promueve la coherencia normativa y la coordinación regional para la efectividad de las políticas, mediante la adopción de estándares abiertos y la neutralidad tecnológica con la participación y corresponsabilidad de los distintos actores del ecosistema digital. El objetivo 28 busca coordinar acciones orientadas a garantizar la privacidad, la protección de datos personales, la defensa del consumidor en línea, el acceso a la información pública y la libertad de expresión, en el entorno digital, evitando el uso indebido y no autorizado de los datos, y fortaleciendo los mecanismos de colaboración entre las autoridades competentes de la región. El objetivo 29 señala la necesidad de mejorar la medición de la transformación y la economía digitales, reforzando los procesos de recolección de datos para las estadísticas oficiales, que incluya el uso de tecnologías avanzadas, el fortalecimiento y la armonización de marcos comunes de indicadores y su monitoreo a través de observatorios sobre la sociedad de la información. Finalmente, el objetivo 30 dispone la importancia de fortalecer la cooperación regional, como un mecanismo esencial para aprovechar las oportunidades y enfrentar los desafíos de la región en materia de la sociedad de la información.

A efectos de cumplir con las líneas de acción y los objetivos, el 13 de julio de 2018 se aprobó el Programa de Actividades de Cooperación Regional de la Agenda Digital para América Latina y el Caribe[53], el cual contiene el detalle de la propuesta, su descripción, los plazos de ejecución y los responsables.

(IV.3.) Agenda Digital Mercosur

En línea con la tendencia internacional, en diciembre de 2017, el Consejo Mercado Común aprobó la Decisión Nº 27/17 - Agenda Digital del Mercosur, por medio de la cual dispone crear el Grupo Agenda Digital (gad), como órgano auxiliar dependiente del Grupo Mercado Común (gmc), con el objetivo de promover el desarrollo de un Mercosur Digital.

53 Programa de Actividades de Cooperación Regional de la Agenda Digital para América Latina y el Caribe, 2018-2020. URL: https://www.cepal.org/sites/default/files/static/files/programa_de_actividades_elac2020_0.pdf Consultado el 15 de enero de 2019.

Asimismo, señala que deben presentar una propuesta de Plan de Acción "Agenda Digital del Mercosur" de plazo bienal, con propuestas de políticas y de iniciativas comunes, con plazos y metas para su ejecución en temas vinculados a la digitalización.

La primera reunión del gad fue en abril de 2018, previendo la aprobación de un Plan de Acción bienal, 2018-2020 "Agenda Digital del Mercosur". En dicho año se reunieron en cuatro oportunidades, y se plantearon los siguientes ejes de acción: *Eje A.* Infraestructura digital y conectividad; *Eje B.* Seguridad y confianza en el ambiente digital; *Eje C.* Economía digital; *Eje D.* Habilidades digitales; *Eje E.* Gobierno digital, gobierno abierto e innovación pública; *Eje F.* Aspectos regulatorios; *Eje G.* Coordinación en Foros Regionales e Internacionales; y *Eje H.* Medición de indicadores.

En la reunión celebrada en octubre de 2018 se trabajó en cinco mesas de trabajo: 1. infraestructura digital; 2. seguridad y confianza; 3. economía digital; 4. habilidades digitales; y 5. gobierno digital.

Asimismo, surge del Acta Mercosur/gad/ Nº 04/18, IV Reunión del Grupo de Agenda Digital, de octubre de 2018, que Argentina informó sobre el proceso de elaboración de la Agenda Digital Nacional, que Brasil comentó sobre los avances en la Estrategia brasilera de Transformación Digital y sobre la Estrategia de Gobernanza Digital, que Paraguay destacó la construcción de la Agenda Digital que próximamente se aprobaría, y que Uruguay compartió el proceso de implementación y evaluación de la cuarta Agenda Digital.

Específicamente, en lo que respecta al Eje de Habilidades Digitales, conforme surge del Acta IV GAD de octubre de 2018, la Delegación de Argentina presentó un documento en el cual dispone la necesidad de generar nuevos modelos educativos para atender y desarrollar las competencias que servirán de herramientas para los nuevos retos. Asimismo, señalan que la política pública educativa es prioritaria y se pone como ejemplo la agenda educativa en Argentina, la cual contempla como prioritarias las denominadas habilidades del Siglo XXI, dentro de ellas: la alfabetización digital, la programación y robótica, las ciencias, tecnologías, ingeniería y matemáticas (STEM).

En esta línea, proponen incorporar a la Agenda una Planificación de Formación en Habilidades Digitales, que permita a la región posicionarse; para lo cual consideran relevante contar con equipos formados, promoviendo el desarrollo regional en

diferentes tecnologías, potenciando los cuadros profesionales, así como las sinergias con empresas y organizaciones.

Por otra parte, se generó un cuestionario sobre ciberseguridad para ser complementado por los países, a fin de realizar un relevamiento de información, previo a la convocatoria de las autoridades competentes.

Como próximas acciones se prevé avanzar en reuniones virtuales de autoridades en los siguientes temas: (i) protección de datos personales, (ii) ciberseguridad, (iii) habilidades digitales, y (iv) gobierno digital y gobierno abierto.

(IV.4.) Agenda Digital de España

Fue aprobada en el año 2013 por el Consejo de Ministros, en el marco de las acciones que el Gobierno de España quiere impulsar para el desarrollo de la economía digital y de la sociedad, estando a cargo del Ministerio de Energía, Turismo y Agenda Digital.

El objetivo es trasladar los beneficios de las nuevas tecnologías a todos (ciudadanos, empresas y Administración) a través del desarrollo de la economía digital, de la reducción de costos de gestión, de la mejora de los servicios al ciudadano, del fortalecimiento del sector TIC y del impulso a la investigación, al desarrollo y a la innovación (I+D+I).

Dispone la hoja de ruta para cumplir con la Agenda Digital Europea y establece seis objetivos al 2020: (1) Despliegue de redes y servicios: se desarrolla junto con la estrategia nacional de redes ultrarrápidas, se pretende que haya una cobertura de más de 30 Mbps para todos y que como mínimo, la mitad de los hogares, tengan una velocidad superior a 100 Mbps. (2) Economía Digital: incentivar a las empresas a adoptar las TIC para mejorar su competitividad, para que puedan expandirse apalancándose en el comercio electrónico, en la producción y en la distribución. (3) E-Administración: alcanzar una Administración Pública más eficiente a través de soluciones digitales, que presten servicios públicos más ágiles, optimicen el gasto, superando la brecha digital. (4) Confianza: se impulsa que se confíe en el ámbito digital, para lo cual es fundamental desarrollar la ciberseguridad, generando entornos más seguros. (5) Investigación, Desarrollo e Innovación (I+D+I): fomentarlo, así como captar más inversiones públicas

y privadas para su impulso. (6) Inclusión digital y empleo: la alfabetización digital busca mejorar la capacitación en el ámbito de las TIC.[54]

Se hace énfasis en el impacto que tienen las TIC para la economía, al respecto, haciendo referencia a datos de la Comisión Europea[55], se indica que el sector TIC representa el 5% del PIB europeo y que un incremento del 10% en la banda ancha genera un incremento entre el 0,9 y 1,5% del PIB. Por otra parte, se hace énfasis en que por cada millón de euros que se inviertan en TIC, se generan hasta 33 puestos de trabajo, que la implementación de la Agenda Digital para Europa va a permitir que se creen 1,2 millones de empleos a corto plazo y 3,8 millones a largo plazo. En lo que respecta a la productividad, se destaca que el sector TIC contribuye al 50% del crecimiento de la productividad; al tiempo que se beneficia el bienestar del consumidor como consecuencia del desarrollo del comercio minorista.

Para la implementación de la agenda, se establecieron diversos planes de actuación[56].

Hay tres planes transversales: (1) el desarrollo de redes ultrarrápidas, (2) investigación, desarrollo e innovación en TIC, y (3) desarrollar la confianza digital; y seis planes específicos, uno enfocado en la ciudadanía, tres con foco en las empresas y dos orientados en la Administración.

En lo que respecta a los ciudadanos, además de que tengan acceso a redes ultrarrápidas, I+D+I y tengan confianza, es esencial trabajar sobre la inclusión digital.

En relación con las empresas, al igual que en los ciudadanos, es fundamental que tengan acceso, que I+D+I y que confíen; al tiempo que es necesario que puedan apalancarse en el comercio electrónico, que puedan internacionalizarse, así como desarrollar contenidos digitales.

Finalmente, en relación con la Administración, además de tener un rol de suma importancia para que todo lo anterior se pueda alcanzar con éxito, también es esencial que trabaje en el desarrollo de la Administración electrónica y en el despliegue de servicios públicos digitales.

---

[54] Agenda Digital para España. URL: https://comparaiso.es/manuales/agenda-digital Consultado el 1 de junio de 2019.

[55] Agenda Digital para España, URL: https://www.lamoncloa.gob.es/documents/agendadigital150213.pdf Consultado el 1 de junio de 2019.

[56] Agenda Digital para España. Idem.

En vista de lo anterior, se quiere fomentar la inversión en redes ultrarrápidas, facilitando el despliegue de las nuevas tecnologías, así como promoviendo la competencia entre las diversas plataformas. Para ello se busca dictar una nueva Ley General de Telecomunicaciones, se desarrolla una estrategia nacional para el desarrollo de redes ultrarrápidas, teniendo como base la compartición de infraestructuras, la coordinación entre los operadores y la Administración, y el uso eficiente del espectro radioeléctrico, flexibilizando el uso y desarrollando el mercado secundario.

Entre las múltiples iniciativas que se generan con las TIC, se plantean nuevas industrias, como son el *cloud computing* (computación en la nube), ciudades inteligentes, *big data*, así como el desarrollo de especialidades que permitan atender el mercado. Se quiere que España esté a la vanguardia de la innovación y que sea atractivo para realizar inversiones. Para la implementación de estos objetivos, se planteó la necesidad de desarrollar I+D+I en las nuevas industrias, que se adecúe la oferta académica, que se participe en proyectos de financiación de emprendimientos, como pueden ser de capital semilla y de riesgo, y que se establezcan grupos de trabajo con participación público- privado.

Para el desarrollo de la confianza en las TIC, lo cual es fundamental para el desarrollo económico y social del país, se plantea como objetivos que se aumente la utilización de los servicios digitales por parte de las personas y de las pequeñas y medianas empresas. Asimismo, se reconoce la necesidad de mejorar las condiciones de seguridad y de protección de las personas, promoviendo un uso responsable del ciberespacio, tanto por parte de los usuarios como de las empresas. Siendo esencial el desarrollo de la confianza y de la ciberseguridad. A fin de alcanzar los objetivos señalados, se identifica la necesidad de que se modifique la regulación para estimular el mercado, sensibilizar, educar, reforzar las instituciones que trabajan en la ciberseguridad, mejorar las condiciones para la realización de transacciones en el medio digital, así como fomentar las buenas prácticas.

Se busca la inclusión digital, disminuir la brecha y que todas las personas usen Internet. Para esto, se planteó aumentar la cantidad de personas que acceden a los servicios, acrecentar la cantidad de profesionales y atender públicos específicos que puedan tener más dificultades, como pueden ser los mayores de 65 años, quienes tienen rentas bajas, quienes están desempleados o tienen muy bajos niveles de estudios. En vista de lo anterior, se propuso trabajar para que la población pueda tener las

habilidades digitales necesarias para poder acceder y usar de la mejor forma Internet, facilitar el acceso a los servicios públicos, captar inversión pública y privada, y sacar provecho de las facilidades que el acceso y los nuevos dispositivos inteligentes pueden ofrecer.

Las pequeñas y medianas empresas tienen la oportunidad de mejorar su productividad y su competitividad utilizando las nuevas tecnologías. A estos efectos, se busca que realicen un uso eficiente de las nuevas tecnologías, que implementen la facturación electrónica y que se apalanquen en el comercio electrónico. Para alcanzar dichos objetivos, se propone establecer centros que muestren cómo utilizar las TIC para determinados sectores, que haya más formación en comercio electrónico y en marketing digital, que haya interoperabilidad entre los sistemas, así como brindar apoyo y asesoramiento a los comerciantes para que puedan comprar y vender a través de Internet.

Ante la necesidad de que las empresas españolas de base tecnológica tengan visibilidad y presencia a nivel internacional, se plantea que se incremente la capacidad de las pequeñas y medianas empresas para poder competir, que aumenten su presencia en el exterior y que aumenten las exportaciones. A estos efectos, se trabaja en el desarrollo de ofertas que sean competitivas, se apoya la internacionalización y se acompaña a las empresas.

La industria de contenidos digitales tiene un gran potencial de crecimiento y contribuye con la economía digital. Para el desarrollo de esta industria, se plantea como objetivo establecer una estrategia integral, que haya actuaciones tanto para los sectores tradicionales como para los nuevos entornos, contribuir para que la industria madure y se consolide, y buscar el crecimiento del sector. Para lo anterior, se busca que crezca el número de centros que ofrezcan formación en estos temas, que se creen foros que contribuyan con el desarrollo de la industria, que se abran programas de exportación e internacionalización, así como que se reutilice la información del sector público en sectores estratégicos, como puede ser el turismo.

La Administración tiene la posibilidad y la necesidad de ser más eficiente y también el desafío de desarrollarse electrónicamente. Para esto se tiene como objetivos que la Administración esté más cerca de los ciudadanos y de las empresas, que se utilice más la administración electrónica, que se racionalice y optimice el uso de las TIC en la Administración, que haya más colaboración y que se rompa la brecha digital. Para estos

fines, se busca racionalizar las estructuras, los procesos, los procedimientos, que se reutilicen los recursos y los servicios.

Asimismo, se quiere impulsar la digitalización de los servicios públicos a fin de conseguir mayor eficiencia, que se extiendan los servicios a todos los ciudadanos, que se impulse la industria TIC y la economía digital. Como actuaciones para alcanzar dichos objetivos, se dispuso: (i) que se desarrolle la justicia digital, implantando la gestión procesal y los expedientes judiciales electrónicos; (ii) que el bienestar social y la salud puedan desarrollarse, extendiendo la receta electrónica y el acceso a la historia clínica a través de internet; y (iii) dotar a los centros de educación de conectividad ultrarrápida para poder alcanzar la educación digital.

A los efectos de cumplir con todo lo anterior, se establece un modelo de gobernanza con tres bases: (1) coordinación entre los diferentes agentes involucrados, (2) ejecución, en base al liderazgo, a la coordinación con expertos y a la colaboración público-privada, y (3) seguimiento y medición.

El Observatorio Nacional de las Telecomunicaciones y de la Sociedad de la Información (ONTSI), en colaboración con el sector público y privado, elabora estudios, realiza el seguimiento y evalúa las políticas públicas, y realiza métricas sobre la Sociedad de la Información en España.

En este sentido, publica anualmente un Informe "La Sociedad en Red" con el objetivo de ofrecer una foto de la situación a dicho momento de la Sociedad de la información en España. En el último informe publicado, Edición 2018, informe anual 2017[57], se concluye, entre otras cosas, que:

Hay un crecimiento constante a nivel nacional e internacional en lo que respecta a los indicadores de la sociedad de la información y al mercado de las TIC.

Los equipos y la conectividad móvil es lo que más crece. La telefonía fija decrece y la banda ancha fija, si bien crece, lo hace en menor medida que la banda ancha móvil.

El avance no es parejo en todas las comunidades autónomas, hay un mayor desarrollo en Madrid, en País Vasco y en Cataluña.

Las microempresas y las grandes compañías crecen en los indicadores de uso.

[57] La Sociedad en Red, Informe Anual 2017, Edición 2017, URL: https://www.ontsi.red.es/ontsi/sites/ontsi/files/La%20sociedad%20en%20red.%20Informe%20anual%202017%20%28Edici%C3%B3n%202018%29.pdf . Consultado el 1 de junio de 2019.

La administración electrónica también se consolida y se trabaja en el Plan Nacional de Ciudades Inteligentes, el cual se centra en: (a) acciones territoriales, como son: conectividad 5G, laboratorios, interoperabilidad, turismo inteligente; (b) acciones de soporte, como son: la normalización, comunicación, capacitación y difusión; y (c) acciones complementarias, como es el desarrollo de Internet de las Cosas.

En relación con las tendencias para el próximo año, se destaca como principales corrientes:

El crecimiento de tecnologías como la Inteligencia Artificial, sobre todo en el uso de chatbots.

El aprendizaje automático o de máquinas, permitiendo que los sistemas aprendan y mejoren la experiencia, sin programación explícita.

La irrupción de blockchain, facilitando la realización transacciones de manera más transparente, segura y descentralizada.

La ciberseguridad, principalmente con la aplicación del Reglamento General de Protección de Datos.

Conectividad total con la tecnología 4G, comenzando el desarrollo de la tecnología 5G.

(IV.5.) Agenda Digital de Uruguay

Fue aprobada por el Decreto Nº 459/016 de 30 de diciembre de 2016 con el objetivo de dar continuidad al fortalecimiento de las políticas digitales de Uruguay, y a los compromisos asumidos en el marco de la Cumbre Mundial de la Sociedad de la Información y la Conferencia sobre la Sociedad de la Información para América Latina y el Caribe.

Interesa destacar que Uruguay es parte del "D9", que engloba a los países más digitalizados del mundo, grupo que incluye a Israel, Estonia, Corea del Sur, Nueva Zelanda, Reino Unido, Canadá, México, Portugal y Uruguay.

Se enmarca en el objetivo de avanzar en la transformación digital del país de forma inclusiva y sustentable, con el uso inteligente de las tecnologías, a fin de que las personas puedan aprovechar al máximo los beneficios de la sociedad de la información y del conocimiento, en igualdad de oportunidades.

Se manifiesta que se considera como altamente positivo el disponer de un instrumento de política que permita priorizar, articular y difundir acciones para establecer una visión de conjunto alineada con los objetivos estratégicos de desarrollo del país, en la que convergen esfuerzos de diversos actores del sector público, del privado, de la academia, de la sociedad civil organizada, así como la comunidad técnica.

La propuesta fue presentada por la Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento (agesic), bajo la consigna "Transformación con equidad", a partir de las distintas iniciativas propuestas por instituciones públicas y privadas.

En este sentido, se aprobó la Agenda y se encomendó a agesic el seguimiento y la evaluación del avance.

A modo de antecedente, la Agenda busca asegurar el acceso de la población a las tecnologías digitales y reducir las brechas digitales, en línea con las anteriores agendas de los años 2008, 2010 y 2015, en base a las cuales se avanzó en el desarrollo de infraestructura y de cobertura. Señalan que el país tiene una amplia cobertura de infraestructura de telecomunicaciones, todos los niños de la educación pública tienen su propia computadora con Internet (Plan Ceibal), se trabaja en que toda la población cuente con competencias básicas de alfabetización digital, se ha implementado la trazabilidad bovina, se ha avanzado en el gobierno digital y en la historia clínica electrónica nacional.

Se busca alcanzar la transformación digital, se quiere trascender el despliegue de infraestructura y herramientas tecnológicas para mejorar y apoyar los métodos tradicionales. Para ello se persigue ampliar la capacidad de innovación, desarrollar el país y contribuir al logro de los Objetivos mundiales establecidos en la Agenda de Desarrollo Sostenible a 2030 por Naciones Unidas.

Se consideran como factores críticos los siguientes: i. el fortalecimiento de habilidades específicas; ii. la incorporación plena de la tecnología en los sectores productivos; iii. la profundización del vínculo entre la ciudadanía y el Estado; y iv. contar con un marco habilitante para su desarrollo.

La Agenda se construye sobre cuatro pilares.

El primer pilar, es vinculado a "Políticas Sociales e Inclusión", destacando la necesidad de disminuir las brechas digitales generadas por la adquisición desigual de

competencias, motivando el interés y la formación de habilidades cada vez más sofisticadas.

Para esto se establecen dos objetivos. El primero relacionado con el desarrollo de habilidades digitales, se indica la necesidad de intensificar la adopción de capacidades digitales avanzadas en la población, incluyendo la formación de recursos calificados en tecnologías digitales. El segundo, vinculado con la innovación, se señala que se deben hacer esfuerzos integradores en la educación, en la salud, en el desarrollo social, en el empleo y en la cultura, así como en el acceso oportuno y descentralizado a la información y a servicios públicos de calidad.

El segundo pilar, busca el "Desarrollo Económico Sustentable". Se reconoce que las tecnologías digitales modifican el desarrollo económico, en tanto inciden en la forma de producir, distribuir y consumir.

Para esto, se establecen tres objetivos. El primero relacionado con la inversión estratégica en infraestructura. Se reconoce que se debe fortalecer la infraestructura para universalizar el acceso y alcanzar mejoras en capacidad y calidad. El segundo objetivo, está vinculado con la economía digital y la innovación para la competitividad. Se dispone que se debe promover la economía digital, creando mayor valor agregado, impulsando la transformación digital de las micro, pequeñas y medianas empresas, buscando aumentar la productividad, el crecimiento y la innovación en los sectores productivos. Por otra parte, el tercer objetivo trata sobre la gestión inteligente de la información ambiental y de emergencias, a efectos de mejorar la capacidad de prevención, mitigación y atención de impactos ambientales y de emergencia, monitoreando los recursos naturales y gestionando la probabilidad de ocurrencia de fenómenos naturales.

El tercer pilar, es la "Gestión de Gobierno". Se parte de la base de que se ha modernizado la gestión pública incorporando tecnología en los procesos, pero señalan que también deben gestionarse y utilizarse estratégicamente los datos, habilitar la incorporación de tendencias digitales y tecnologías emergentes para crear valor público, innovando en la toma de decisiones y en la adopción de nuevos modelos de relacionamiento con la ciudadanía.

En esta línea, se disponen dos objetivos. El primero es alcanzar un gobierno de cercanía, como una manera distinta de entablar la relación entre los ciudadanos y el

Estado, promoviendo la transparencia, la rendición de cuentas, la participación de la ciudadanía y el desarrollo de mejores servicios. El segundo busca un gobierno integrado e inteligente, a fin de avanzar hacia un Estado que actúe como una unidad e intensificar el aprovechamiento de los datos para la toma de decisiones, la orientación de políticas públicas, mediante servicios proactivos que se anticipen a las necesidades.

Finalmente, el cuarto pilar, es sobre la gobernanza para la sociedad de la información, la cual se desarrolla en forma dinámica, descentralizada y en múltiples dimensiones que desafían la articulación y la colaboración.

Al respecto, se establecen dos objetivos. El primero relacionado con la confianza y la seguridad en el uso de las tecnologías digitales, construyendo entornos que promuevan la plena participación de la sociedad. Es interesante destacar que, entre los compromisos, se dispone el adecuar el marco normativo en protección de datos personales, cibercrimen, e-Residuos y protección del e-Consumidor; asimismo, se dispone articular acciones mediante un Centro Nacional de Operación de Ciberseguridad, desarrollar un plan para sensibilizar sobre el buen uso de Internet, alcanzar al 30 % de la población con mecanismos de identidad electrónica y que toda la Administración Central cumpla los requerimientos mínimos de ciberseguridad y continuidad operativa. Como último objetivo, se establece producir estadísticas TIC nacionales, para fortalecer los marcos institucionales para monitorear, medir y promover el sector TIC, al tiempo que sirvan para adecuar las políticas digitales y los procesos de toma de decisiones.

Para la ejecución de la Agenda, sin perjuicio de que para cada objetivo se identifican a diversos organismos responsables, se creó el Consejo para la Sociedad de la Información; órgano que orienta los procesos de elaboración y priorización, al tiempo que monitorea y evalúa las iniciativas. Asimismo, se previó para una evaluación intermedia la posible creación de un centro de investigación nacional en informática, así como incluir la computación como materia en la formación secundaria.

Por otra parte, se prevén monitoreos y evaluaciones, mediante: (i) el seguimiento trimestral de los indicadores, (ii) convocando semestralmente al Consejo para discutir los avances, (iii) realizando reportes anuales, y (iv) promoviendo la discusión con todas las partes interesadas en el Foro de Gobernanza de Internet de Uruguay.

El grado de avance de cada una de las metas se puede seguir en la siguiente página web: www.uruguaydigital.uy.

V. Retos y oportunidades regulatorias

Como surge de lo anterior, son múltiples los desafíos que esta nueva realidad digital conlleva para todos los ciudadanos, para las empresas y para las administraciones públicas.

La transformación digital impacta en todo, y mientras las personas –que somos quienes estamos atrás de las empresas, de los organismos y de los reguladores- pensamos de manera lineal -así nos educaron, de esa forma solemos explicar las gráficas, los crecimientos, etc.-, la tecnología evoluciona de forma exponencial. Se están generando grandes diferencias entre aquellos que responden adecuadamente, innovan y son capaces de ejecutar los cambios; respecto de los "tradicionales", que se siguen aferrando a lo conocido o que aún no han tenido tiempo para adaptarse o para ejecutar los cambios.

En la nueva realidad el modelo vertical se integra, gracias a la interoperabilidad, lo cual permite: manejar de forma más adecuada la información, acelerar los procesos, facilitar las transacciones; lo cual se traduce en: más eficiencia, más simplicidad, menos costos, menos tiempo y menos errores.

En este nuevo escenario, ingresan nuevos actores, que fragmentan partes de los clásicos procesos y negocios, se especializan en una parte de la cadena, innovan e impactan en el valor de la industria tradicional.

Lo anterior lo vemos en múltiples industrias. A modo de ejemplo: en la banca, en el entretenimiento y en las telecomunicaciones.

Ante este nuevo escenario, todos tenemos grandes retos y sin duda muchas oportunidades, siendo el tiempo un factor clave. Es esencial actuar de forma ágil para poder transformarse y competir adecuadamente; así como observar y medir constantemente la evolución, los resultados de la innovación adoptada, y obrar en consecuencia para que la digitalización realmente se universalice y todas las personas sean capacidad de adaptarse y puedan ser parte.

En este escenario tan cambiante y en donde todo ocurre a grandes velocidades, actuar con diligencia es fundamental, pero hay que tener cuidado porque todos los

países tienen ante esta nueva realidad grandes oportunidades de desarrollo, y una regulación inadecuada no solo puede afectar la innovación y el desarrollo, sino que además puede generar inseguridad y como consecuencia derivar en la pérdida de inversiones, de talentos y en consecuencia, de desarrollo e innovación, con todo el impacto que eso puede conllevar para una sociedad.

Cada vez es más necesario: (i) simplificar, (ii) escuchar, (iii) identificar los riesgos y los problemas, (iv) crear valor, (v) adaptarse para acompañar la transformación, (vi) promover la innovación, la investigación y el desarrollo, (viii) comprender que los modelos cambiaron, que los límites entre los diversos mercados en muchos casos se borraron y que hay nuevos competidores, (ix) educar y proteger a los consumidores, (x) actuar con diligencia y celeridad, mas con cautela, una mala regulación, que limite la innovación y la inversión, puede generar una avalancha de perjuicios para cualquier sociedad.

En vista de lo anterior, no cabe duda de que los Reguladores tienen grandes desafíos, pero también pueden contribuir mucho en el adecuado desarrollo, impulsando la innovación, otorgando previsibilidad y contribuyendo directamente para poder captar inversiones.

Como señala la Dra. Cristina Vázquez[58]:

- El Regulador es clave para el equilibrio.
- *"La Regulación no es un proceso simple" (...) "sino una red de relaciones en la que cada parte procura obtener la satisfacción de su interés, resultando imposible que un gripo consiga lograrlo plenamente*"[59].
- La teoría y la experiencia recomiendan el fortalecimiento de estas entidades: más presupuesto, más capacitación, más independencia.
- Los cometidos se concretan mediante leyes y se complementan con actos administrativos de la regulación específica.
- *"Los principales obstáculos que debe sortear la regulación con vistas a la obtención de sus objetivos, tienen que ver con las dificultades para la*

[58] VÁZQUEZ, CRISTINA, "Desafíos regulatorio ante la digitalización" en *"Estudios sobre los Desafíos Jurídicos ante la Digitalización"*, Universidad de Montevideo, 2018, pp. 57 y ss.
[59] VAZQUEZ, CRISTINA, obra citada, pp. 76..

obtención de información, los riesgos de "captura del Regulador", sea por la política o los agentes regulados, y la fragilidad del apoyo del consumidor.[60]*"*

- Se deben tener en cuenta los objetivos de la regulación, teniendo como principal la protección de los derechos de los usuarios o consumidores, y como secundarios: la sostenibilidad, la eficiencia y la equidad.

- Toda regulación debe atender el principio de proporcionalidad, lo cual implica analizar la idoneidad, la necesidad y ponderar.

Entre los diversos retos que la nueva realidad plantea a los Reguladores, siguiendo lo señalado por la Dra. Vázquez[61], se destacan:

- El ritmo: *"Los nuevos marcos deben producirse en tiempos mucho más acotados e irse adecuando permanentemente mientras se sigue trabajando con los vigentes*[62]*."*, al tiempo que presentan "*el peligro de regulaciones dictadas con premura y de manera no meditada. Es así como ambos extremos –el de la lentitud y el de las prisas– deben evitarse*[63]*".*

- Regulaciones fragmentadas y superpuestas: es necesario que haya coordinación.

- Respectar los límites regulatorios: no cruzar a otras categorías regulatorias, hay que prestar atención a las zonas grises.

- La privacidad y la seguridad digital: buscar el justo equilibrio entre el acceso a la información y la protección de los datos personales.

- La "caja negra" y los sesgos algorítmicos: atender el uso de la inteligencia artificial y de los algoritmos en la toma de decisiones.

En vista de lo anterior, teniendo en cuenta que la nueva realidad impacta en todo, a todos, a una velocidad exponencial, y que la innovación y el desarrollo juega un rol esencial para el despliegue de las nuevas tecnologías, cada vez toma más relevancia otorgar seguridad, previsibilidad y reglas claras, siendo esencial que la forma de regular se adapte, en tanto:

---

[60] Ibidem.
[61] Ibidem.
[62] Ibidem.
[63] Ibidem

El cambio es constante y es cardinal comprender los aspectos técnicos y del negocio, si se regula sin entender cabalmente el supuesto se corren grandes riesgos de limitar sin fundamento, afectando el desarrollo y la innovación.

La flexibilidad y la adaptabilidad es básica, hay que revisar la regulación vigente y la que se dicte, puede ser que lo vigente no refleje la realidad, los principios generales de derecho toman cada vez más importancia, así como las guías, las recomendaciones y la autorregulación.

Previo a regular es importante identificar qué es lo que se quiere regular, cuál es el riesgo o el problema que se quiere atender, o cuales son los aspectos de sostenibilidad, de eficiencia o de equidad que requieren atención.

Se tiene que atender el principio de proporcionalidad, y considerar si la medida vigente o la propuesta es idónea, es necesaria y si está ponderando adecuadamente los diversos derechos o intereses en juego.

Hay que tender a la regulación colaborativa, dialogando, escuchando, así como al desarrollo de *sand boxes* a efectos de analizar en conjunto el fenómeno y atender aquellos aspectos que lo requieran.

Es fundamental analizar la nueva realidad en su globalidad, no podemos responder adecuadamente a la misma, si en realidad lo que hacemos es pretender que se ajuste a regulaciones pensadas para supuestos completamente diferentes.

Tender a las regulaciones ex post, reforzar las herramientas de control, el acceso a la información, la transparencia y el trabajo colaborativo.

En suma, como señala la Dra. Vázquez: *"la nueva regulación debe escoger su rol entre convertirse en obstáculo o motor de la innovación. A efectos de colocarse en este segundo papel, el Regulador debe desarrollar su actividad de manera ágil, iterativa y colaborativa, atendiendo a los resultados y ambientando el ensayo de nuevos modelos en entornos controlados."*[64]

VI. Consideraciones finales

La digitalización tiene un rol clave en el ámbito social y económico, generando múltiples oportunidades y desafíos que plantean, al ordenamiento jurídico, el reto de adaptarse y de responder adecuadamente al nuevo contexto.

[64] VÁZQUEZ, CRISTINA, obra citada, pp. 81.

La revolución digital y la transformación que conlleva es un proceso que ha ido evolucionando y que se ha ido integrando, gracias al desarrollo que han tenido las telecomunicaciones, las plataformas y las diversas tecnologías; y que, gracias a la globalización, se ha universalizado, siendo cada vez más asequible y accesible.

Sin perjuicio, aún resta mucho por hacer. Es esencial adoptar medidas para disminuir la brecha digital y conectar a todos, al tiempo que proteger los derechos fundamentales de las personas –como ser su seguridad, su privacidad, la igualdad y su libertad de expresión–, y promover la competencia, la innovación y el desarrollo.

La nueva realidad digital ofrece un sinfín de oportunidades y de beneficios para la sociedad, mas también presenta múltiples retos que las sociedades, actuando en conjunto, deben afrontar. Una buena muestra de cómo se está trabajando en la temática, son las agendas digitales –tanto a nivel regional, como a nivel país–, dado que muestran los diversos elementos del ecosistema que se tienen que desarrollar a fin de alcanzar la transformación digital de la mejor manera.

En este contexto, el Derecho y los reguladores tiene muchos desafíos en tanto herramienta para garantizar que los derechos que las personas y las empresas tienen en el mundo offline o tradicional también los detenten en el mundo *online* o digital. Al tiempo que, en un escenario tan cambiante, donde se generan profundas modificaciones económicas y sociales de manera vertiginosa, los principios fundamentales toman cada vez mayor relevancia; siendo esencial analizar y atender la nueva realidad en su globalidad, no podemos responder adecuadamente a la misma, pretendiendo que se ajuste a regulaciones o a situaciones pensadas para supuestos completamente diferentes.

El cambio es continuo, es cardinal comprender los aspectos técnicos y del negocio, así como el trabajo colaborativo y el dialogo constante entre las diversas partes. La flexibilidad y la adaptabilidad es básica, hay que revisar la regulación vigente y la que se dicte, puede ser que lo vigente no refleje la realidad. Previo a regular es importante identificar qué es lo que se quiere regular, cuál es el riesgo o el problema que se quiere atender, o cuales son los aspectos de sostenibilidad, de eficiencia o de equidad que requieren atención. Asimismo, hay que observar si las medidas propuestas son proporcionales, idóneas y necesarias para el fin buscado.

La regulación debe ser un elemento que contribuya con la innovación, con el desarrollo, que otorgue previsibilidad y que permita captar inversiones; para lo cual, es

esencial que se desarrolle de forma colaborativa con el mercado, dando seguridad, transparencia y reglas claras.

En suma, la revolución digital plantea múltiples oportunidades y desafíos que necesariamente debemos atender, esta nueva realidad impacta en todos y en todo, a gran velocidad, y permite acelerar el logro de los Objetivos de Desarrollo Sostenibles, aprobados por las Naciones Unidas para 2030. Mas sin duda, lo anterior requiere de diversas actuaciones que se deben coordinar, controlar y ajustar, a nivel nacional, regional e internacional, a efectos de poder cumplir cabalmente con los fines buscados.

CAPÍTULO II: LAS REDES DE TELECOMUNICACIONES Y LOS NUEVOS PARADIGMAS REGULATORIOS

I. Introducción

Estamos ante una revolución digital de gran impacto social y económico, que cambia todo, a velocidades exponenciales, generando una nueva realidad, la digital, que se desarrolla sobre las redes de telecomunicaciones.

La digitalización presenta múltiples desafíos, y por el impacto que genera en los derechos de las personas y en la economía, cada vez más se analiza la regulación de las TIC y la Gobernanza de Internet.

Las redes de telecomunicaciones, principalmente Internet, junto con el gran desarrollo de la tecnología y la convergencia, son esenciales para que la transformación digital se pueda desarrollar debidamente, en tanto son la espina dorsal sobre las cuales se desarrolla todo el ecosistema digital.

Estamos en un momento de constantes cambios, donde el Derecho y la Regulación juegan un rol esencial para dar seguridad, transparencia y previsibilidad. Una mala regulación o que no se ajuste a la realidad, puede afectar mucho a una sociedad, en tanto puede limitar la innovación, el desarrollo, la investigación y desestimular la inversión.

En este nuevo contexto, tan cambiante, se presentan constantemente nuevas formas de hacer las cosas, muchas de las actividades que antes realizábamos de forma *offline*, en el mundo físico, ahora se pueden hacer a través de diversas plataformas electrónicas, digitales, de forma automática y algunas incluso a través de robots.

Estos cambios ocurren en las más diversas áreas de actividad, modificando los modelos de negocios, así como la forma en que se prestan y consumen los servicios.

En este sentido, gracias a la convergencia, al gran desarrollo de Internet y de las nuevas tecnologías, la forma en que se prestan los servicios de telecomunicaciones también cambió, y la regulación vigente en muchos casos atiende un modelo que poco tiene que ver con la realidad.

No podemos pretender responder adecuadamente a una nueva realidad, intentando que la misma encaje en supuestos pensados para realidades diferentes. La tecnología va más deprisa que la regulación, no tiene sentido alguno pretender "estirar" supuestos de regulación, algunos de modelos vetustos, a nuevas modalidades, las cuales difícilmente hayan podido ser imaginadas a la hora de dictar las normas.

Hay que analizar los supuestos de manera cabal, buscando las respuestas en los principios generales, dejando sin efecto lo que ya no sea necesario, actualizando lo que se requiera y poniendo en el centro a las personas, así como al desarrollo social y económico de todos.

En el presente capítulo trataremos sobre las redes de telecomunicaciones, profundizaremos en Internet, comentaremos sobre los nuevos paradigmas regulatorios y sobre diversos modelos y niveles de gobernanza.

II. Redes de telecomunicaciones

El despliegue de redes de telecomunicaciones se presenta como uno de los pilares fundamentales para el desarrollo del mundo digital.

La Unión Internacional de Telecomunicaciones, define las redes de telecomunicaciones como el "Conjunto de equipos *(que comprende cualquier combinación de los siguientes elementos: cable de red, equipo terminal de telecomunicaciones y sistema o instalación de telecomunicaciones) indispensables para garantizar el funcionamiento normal de la propia red de telecomunicaciones."*[65], asimismo como: "*Red que, en virtud de una licencia concedida por una autoridad nacional de telecomunicaciones, presta servicios de telecomunicaciones entre puntos de terminación de red (ntp) (es decir, excluido el equipo terminal más allá de esos puntos)*[66]*",* y finalmente como "*Conjunto de nodos y enlaces que proporciona conexiones entre dos o más puntos definidos para la telecomunicación entre ellos.*[67]"

65 Unión Internacional de Telecomunicaciones, URL: https://www.itu.int/net/itu-R/asp/terminology-definition.asp?lang=es&rlink={03A8C3A6-D1F1-4B8C-B27C-ca20B0139df6} Consultado el 7 de febrero de 2019.

66 Unión Internacional de Telecomunicaciones, URL: https://www.itu.int/net/itu-R/asp/terminology-definition.asp?lang=es&rlink={ff82D1C2-4fed-4078-ac1A-86A470ee75df} Consultado el 7 de febrero de 2019.

67 Unión Internacional de Telecomunicaciones, URL: https://www.itu.int/net/itu-R/asp/terminology-definition.asp?lang=es&rlink={5B1E44ad-78E4-4190-B129-376dea4D2E44} Consultado el 7 de febrero de 2019.

Por su parte, el Diccionario de la Real Academia Española define "Red", entre otras definiciones, como *"7. Conjunto de elementos organizados para determinado fin*[68]*"*, dando como ejemplo la red de abastecimiento de agua o la red telefónica o la red de carreteras, y como "11. *Internet".*

Pasando ya a la definición de "telecomunicaciones", el Diccionario de la Real Academia Española, la define indicando que deriva de "*tele"-1* y de "*comunicación*". Definiendo a "*tele"-1* [69] como: "*a distancia*". Por lo que se entiende que "*telecomunicación*" sería "*comunicación a distancia*". También se define como "*Sistemas de transmisión y recepción a distancia de señales de diversa naturaleza por medios electromagnéticos*".

En sentido técnico, en el Convenio Internacional de Telecomunicaciones de 1973 se definió como *"toda transmisión, emisión o recepción de signos, señales, escritos o imágenes, sonidos o informaciones de cualquier naturaleza por hilo, radioelectricidad, medios ópticos u otros sistemas electromagnéticos*"[70].

Esta definición es la adoptada por el ordenamiento jurídico español y por el uruguayo.

Vale señalar que, en la Ley General de Telecomunicaciones de España, Nº 9/2014, conforme lo establecido en el artículo 1º, se dispone además que las "telecomunicaciones" *"comprenden la explotación de las redes y la prestación de los servicios comunicación electrónicas y los recursos asociados"*.

Como surge del preámbulo de la Ley General de Telecomunicaciones de España N° 9/2014[71]:*"Las telecomunicaciones constituyen uno de los sectores más dinámicos de la economía y uno de los que más pueden contribuir al crecimiento, la productividad, el empleo, y, por tanto, al desarrollo económico y al bienestar social, afectando directamente al círculo de protección de los intereses generales."*

---

68 Diccionario de la Real Academia Española, Definición de Red: URL: https://dle.rae.es/?w=red ◇ consultado el 7 de febrero de 2019.

69 Diccionario de la Real Academia Española, definición de Tele. http://dle.rae.es/?id=zlksvgw|zllzopm Consultado el 28 de octubre de 2017.

70 DELPIAZZO CARLOS, *Lecciones de Derecho Telemático,* Tomo I, Fundación de Cultura Universitaria, Montevideo, 2009, pág. 9.

71 https://www.boe.es/buscar/act.php?id=BOE-A-2014-4950 Consultado el 15 de enero de 2020.

De las definiciones expuestas puede concluirse que las redes de telecomunicaciones son el conjunto de equipos y de sistemas que hacen posible las conexiones a distancia para que se transmita información de cualquier naturaleza, por diversos medios, como ser ondas electromagnéticas o fibras ópticas.

Como señalamos anteriormente, dentro de las definiciones de "Red", la Real Academia Española incluye a "Internet". Si bien, tradicionalmente, Internet o la transmisión de datos es considerado como un tipo de servicio de telecomunicaciones, en la actualidad este servicio toma gran protagonismo, en tanto los servicios tradicionales de telecomunicaciones, como ser los servicios de mensajes de texto o las llamados de voz, son sustituidos y compiten con aplicaciones específicas que se brindan sobre Internet, al tiempo que gracias a la convergencia, también los servicios tradicionales comienzan a ser brindados sobre la red ip, lo cual representa grandes desafíos y genera nuevos paradigmas.

III. Internet

El Diccionario de la Real Academia Española define "*Internet*" como "*Red informática mundial, descentralizada, formada por la conexión directa entre computadoras mediante un protocolo especial de comunicación*"[72].

Con frecuencias las personas utilizan el término "Internet", sin caer en la cuenta de que se compone de "inter" + "net". "Inter" es latín y significa "among" en inglés o "entre" en español; mientras que "net" en inglés es la forma corta de decir "networks", que significa "red" en español. En este sentido, Internet es un sistema que conecta entre sí redes de computadoras individuales, permitiendo la transferencia de datos digitales o de bits, a través de la red. Es básicamente un sistema de telecomunicaciones por redes de computadoras, por lo que a veces se le llama la red de redes[73].

Si bien se pueden encontrar diversas definiciones, como bien indica Internet Society[74], definir Internet no es simple, y "*a diferencia de cualquier otra tecnología, Internet puede ser lo que sea que hagamos. Podemos darle forma. Podemos moldearlo.*

72 Diccionario de la Real Academia Española, Definición de Internet. URL: https://dle.rae.es/?id=LvskgUG Consultado el 7 de febrero de 2019.
73 MURRAY, ANDREW, *Information Technology Law*, Oxford University Press. Oxford, 2016, pp. 16 y ss.
74 Internet Society, URL: https://www.Internetsociety.org/es/Internet/ Consultado el 7 de febrero de 2019.

Pero lo más importante, podemos usarlo para conectar personas, comunidades y países de todo el mundo".

(…) "*consiste en decenas de miles de redes interconectadas operadas por proveedores de servicios, compañías individuales, universidades, gobiernos y otros. Los estándares abiertos permiten que esta red de redes pueda comunicar. Esto hace posible que cualquiera pueda crear contenido, ofrecer servicios y vender productos sin requerir el permiso de una autoridad central*"[75].

Es interesante tener presente cómo fue la evolución de Internet, hay mucho escrito al respecto, mas Internet Society señala que la misma se desarrolló a partir de cuatro aspectos fundamentales: (i) Tecnología, (ii) Infraestructura, (iii) Comunidad, y (iv) Comercialización y difusión de las investigaciones.[76]

En lo que respecta a sus orígenes, a continuación, se comenta brevemente parte de la historia, tomando como base lo publicado por Internet Society en "*Breve Historia de Internet* "[77] y por Andrew Murray[78].

Los primeros pasos hacia lo que es la Internet comenzó en los años 60, por un grupo de visionarios, con la idea de una red de computadoras.

Se suele considerar como puntapié inicial, los trabajos de J.C.R. Licklider, del Massachusetts Institute of Technology (mit). Licklider trabajó sobre la interacción entre las personas y las tecnologías, lo que lo convenció sobre el gran potencial de las interfaces entre personas y computadoras; derivando en el año 1962 con su obra donde describe su concepto de "Red Galáctica", donde imaginó un conjunto de ordenadores interconectados globalmente, a través de los que todo el mundo podría acceder rápidamente a datos y programas desde cualquier sitio.

Vale tener presente que, en octubre de 1957, la Unión Soviética lanzó el primer objeto elaborado por el hombre al espacio, lo cual causó sorpresa a los militares y

---

75 Internet Society, URL: https://www.Internetsociety.org/es/about-the-Internet/how-it-works Consultado el 7 de febrero de 2019.

76 Internet Society, URL: https://www.Internetsociety.org/es/Internet/history-Internet/brief-history-Internet/ Consultado el 8 de febrero de 2019.

77 Internet Society, "Breve Historia de Internet" realizado por Barry M. Leiner, Vinton G. Cerf, David D. Clark, Robert. E. Kahn, Leonard Kleinrock, Daniel C. Lynch, Jon Postel, Larry G. Roberts, Stephen Wolff. URL: https://www.Internetsociety.org/es/Internet/history-Internet/brief-history-Internet/ ◇ Consultado el 9 de febrero de 2019.

78 MURRAY, ANDREW, obra citada, p. 17.

científicos de Estados Unidos, y derivó en que el entonces presidente de ese país, Eisenhower, determinara que Estados Unidos nunca fuera tomado nuevamente por sorpresa en aspectos de tecnología. En consecuencia, se creó una nueva agencia de investigación, que dependía directamente de la oficina del presidente, y se denominó "*Advanced Research Projects Agency*" –Agencia de Proyectos de Investigación Avanzada– o arpa.

Uno de los principales problemas que se enfrentaron fue el ineficiente uso que se hacía de los equipos científicos y que eran muy costosos. Además, usaban técnicas de procesamiento que les requería días introduciendo la información, previo a que el programa pudiera funcionar y luego un error en la entrada de la información invalidaba todo lo hecho. Se vio como solución que los usuarios compartieran los recursos de forma más eficiente, como ser los ordenadores, y crear una red que permitiera a los investigadores en diferentes partes del país compartir los resultados y recursos de manera simple.

Para esto, Licklider, junto con Wes Clark, Bob Taylor, Larry Roberts y Leonard Kleinrock, se dispusieron a crear un sistema de comunicaciones para computadoras, el cual se llamaría "*Advanced Research Projects Agency Network*" –Red de la Agencia de Proyectos de Investigación Avanzada– o arpanet.

Entre los principales hitos, se destaca la teoría de Leonard Kleinrock, del mit, del año 1961, sobre la conmutación de paquetes. Implicaba que un mensaje o una comunicación se dividía en paquetes pequeños, que luego eran direccionados y enviados de forma individual. Una vez que todos los paquetes llegaban a destino, se juntaban nuevamente formando el mensaje original. Esta modalidad de comunicación era más eficiente que la de circuitos, por lo que se implementó en arpa y luego se comenzó a trabajar en la red.

Por otra parte, se enfrentaron a la necesidad de que las computadoras fueran compatibles entre sí, que tuvieran una interfaz, que pudieran comunicarse entre ellas, en esos momentos no había un sistema operativo estándar. Wes Clark dio la solución. En vez de tener que conectar a cada máquina directamente a la red, podían instalar un minicomputador llamado "*Interfaz message processor*" o "IMP" en cada sitio, el cual podría manejar la interfaz entre el ordenador que funcionara como punto inicial o final de la transferencia de datos (*host*) y la red de arpanet. De esta manera, solo se tendría

que escribir la interfaz entre cada ordenador y el imp, el imp usaría el mismo lenguaje y la red del imp se encargaría del resto.

Ya definida la base, Larry Roberts comenzó con el diseño en capas, y finalmente en 1969 la visión de arpanet se hizo realidad cuando un estudiante de ucla, Charley Kline, ingresó al *host* de *Stanford Research Institute* (sri), sds 940, a través del *host* de ucla, Sigma 7. Esos fueron los primeros dos nodos de la red.

Posteriormente, se agregaron dos nodos más. Uno con la Universidad de California en Santa Bárbara con Glen Culler y Burton Fried, que estaban investigando métodos para mostrar funciones matemáticas usando pantallas de almacenamiento, para resolver el problema de la actualización de red. El otro, con Robert Taylor e Ivan Sutherlan, de la Universidad de Utah, que estaban investigando métodos de representación 3D en la red.

De esta manera, a finales de 1969 había cuatro *hosts* conectados en la arpanet inicial. Se entendió como una primera etapa, con la que Internet comenzaba su trayectoria, pero era diferente a la Internet actual, en tanto era una sola red, que se la describía como cerrada.

En los años 70 se comenzó una etapa de gran experimentación. Uno de los primeros experimentos fue con los carriers de telecomunicaciones. arpanet utilizó la red de AT&T, pero fue poco eficiente en las zonas donde no había buena cobertura, como en Hawái. En este sentido, se le solicitó al Profesor Norm Abramson de la Universidad de Hawái que desarrollara una red inalámbrica. Abramson utilizó sus recursos para crear una simple red, denominada “alohanet”, que consistía en siete computadoras alrededor de la isla, que utilizaba radios, similares a la de los taxis, para transmitir y recibir información.

alohanet recibió mucha atención, sobre todo para fines militares, en tanto se percibieron los beneficios de las comunicaciones inalámbricas, mas se advirtió el problema de que la red era limitada y que construir transmisores más grandes, centralizaría la red, dejándola expuesta a ataques.

Así se reparó en la posibilidad de utilizar satélites para desarrollar comunicaciones internacionales, para lo cual Estados Unidos, junto con Inglaterra y Noruega, trabajaron juntos para desarrollar una red satelital, la cual se denominó satnet.

En paralelo, ya en diversos países, como ser Inglaterra y Francia, se estaban desarrollando redes locales fijas; por lo que, al desarrollarse muchas redes independientes, comenzó a crecer el interés de conectarlas, de crear una red de redes.

Había redes satelitales, redes de radios, redes fijas, cada una tenía sus propias reglas, su propio lenguaje, el fin era poder conectarlas a todas, para que se pudieran comunicar entre ellas.

Ante este desafío, Kahn, quien había colaborado a diseñar el imp, empezó a trabajar para poder conectar a todas las redes que se habían ido creando. Se dio cuenta que la dificultad se podía solucionar utilizando una arquitectura de red abierta, lo cual permitía que cada red individual continuara utilizando su arquitectura, mientras que la conexión entre las diversas redes se daba en una capa superior. Para esto se necesitaba un lenguaje común, un protocolo que pudiera ser utilizado por todas las redes.

Aquí se planteó otro inconveniente. En el año 1970 el *Network Working Group* (nwg), liderado por S. Crocker, había creado el protocolo de host a host inicial de arpanet, llamado *Network Control Protocol* (ncp). Tras su implementación, los usuarios de la red pudieron comenzar a desarrollar aplicaciones, pero ncp no tenía la capacidad de dirigirse a otras redes, por lo que Kahn tuvo que desarrollar una nueva versión del protocolo que atendería las necesidades de una red de arquitectura abierta.

En esta línea, creó el Protocolo tcp/ip, el cual se basó en cuatro reglas[79]: *(1) Cada red debería mantenerse por sí misma, y no debería ser necesario hacer cambios internos para que esas redes se conectasen a Internet. (2) La comunicación se haría en base al mejor esfuerzo. Si un paquete no llegaba a su destino final, se retransmitía poco después desde el origen. (3) Se usarían cajas negras para conectar las redes, luego se llamarían puertas de enlace y enrutadores (gateways y routers). Las cajas negras no guardarían información acerca de los flujos individuales de paquetes que pasaran por ellas, manteniendo su sencillez y evitando la complicación de la adaptación y de la recuperación a partir de varios modos de error. (4) No habría control global al nivel operativo.*

79 Breve Historia de Internet, obra citada. URL: https://www.Internetsociety.org/es/Internet/history-Internet/brief-history-Internet/ Consultado el 9 de febrero de 2019.

Kahn comenzó a trabajar con Vint Cerf, quien hizo una analogía con las redes de transporte y sus carriers. Se dio cuenta que los carriers de productos usualmente los cargan sin saber qué hay en ellos. Por ejemplo: transportan un contenedor, que tiene determinados estándares (por ejemplo: tamaño), que puede tener cualquier cosa adentro (por ejemplo: un auto, un mueble, comida), que puede ser trasladado por cualquier red o medio (por carreteras, por tren, por barco, por avión), y nadie de los que lo transportan necesitan saber qué es lo que están cargando, las únicas personas que tienen que conocerlo son el que lo envía y el que lo recibe.

Partiendo de esta analogía, diseñaron el protocolo de transmisión (*Transmission Control Protocol o tcp*), que trabajando de la mano del Protocolo ip, empaquetaban la información y la enviaban por cualquiera de las redes de la familia tcp/ip. El problema que se planteó fue, cómo asegurar que la información llegue a destino y llegue bien. Para asegurar la fiabilidad de extremo a extremo, diseñaron que cuando un paquete de información fuera enviado, llevara con él una solicitud de acuse de recibo. Si el acuse de recibo no llegaba, se retransmitiría el paquete a intervalos aleatorios hasta que se recibiera un acuse de recibo.

Entre 1973 y 1978 el protocolo se siguió mejorando continuamente, se suele decir que lo más importante ocurrió en 1978 cuando Cerf, junto con Jon Postel, publicaron la versión 3 de las especificaciones del protocolo. Esta versión dispuso la división del protocolo en dos protocolos de control de transmisión.

La Internet moderna aún utiliza la familia de protocolos tcp/ip, la información se quiebra en paquetes, se transmiten y se vuelven a juntar al final, asegurándose de que sean dirigidos al destino correcto. Se puede hacer la analogía con el envío de una carta por correo postal.

Como toda comunicación entre redes, se confía en la habilidad de transmitir contenidos de una parte hacia la otra. Para ello, al igual que en la red telefónica donde cada teléfono tiene un número único que lo identifica, en Internet todos los dispositivos que se conecten a la red tienen que tener una dirección o un número único de identificación. Ese número que lo identifica se denomina la dirección ip, es único y esencial para poder hacer la transmisión.

Dentro de las continuas mejoras, actualmente se está migrando de la versión Ipv4 a la Ipv6. La versión Ipv4 consiste en 32 bits, los 8 primeros *bits* individualizan la red,

los otros 24 individualizan el *host* de esa red. No se esperaba la gran universalización que tuvo Ipv4 y se están agotando las direcciones. En consecuencia, se desarrolló el Ipv6, que cuenta con 128 bits y tiene muchas mejoras en relación al Ipv4, manteniendo la compatibilidad "hacia atrás".

Una vez que las computadoras tienen una dirección ip, se puede realizar la transferencia entre ellas. La computadora que origina el envío va a tener el documento o archivo a transmitir y la dirección ip de a dónde la quiere enviar. El protocolo toma ese documento o archivo, lo divide en paquetes, coloca cada paquete en un sobre electrónico y coloca un encabezado con toda la información necesaria para enviarlos al destino correcto y que se rearme al final.

La transferencia se realiza a través de las infraestructuras de las redes de telecomunicaciones, ya sean redes de cobre, de fibra óptica o por medios inalámbricos. En el caso de los medios inalámbricos, las redes pueden ser proporcionadas en áreas locales específicas, por ejemplo: el wi-fi que se proporciona en un café, o en áreas amplias, como puede ser la provista por los operadores de servicios de telecomunicaciones móviles.

Para que el sistema funcione debidamente, de manera universal, se necesitan múltiples redes de telecomunicaciones que se interconecten entre sí y que intercambien el tráfico de paquetes a través de los puntos de acceso a la red, permitiendo que los datos puedan moverse a través de Internet, siendo gestionados a través de *routers* o enrutadores.

Vale destacar que el protocolo ip funciona bajo la base de "mejor esfuerzo"(*best-effort*), lo cual implica: (i) que si hay un archivo dañado o si no pueden encontrar una dirección ip, no se garantiza que se llegue a destino, (ii) que considerando la capacidad de la red, los paquetes se van a enviar de la forma más eficiente posible, y (iii) que la red trata a todos los paquetes de datos de la misma forma.

IV. Nuevos paradigmas regulatorios

Con el desarrollo de las tecnologías, la convergencia digital ha transformado el ecosistema, con múltiples beneficios para los usuarios, en tanto aumenta la competencia, permitiendo que las personas puedan acceder a más servicios, a menores precios.

Los efectos de la convergencia los vemos en las redes, en la forma en que se prestan los servicios, en los dispositivos que utilizamos, así como en la gran variedad de contenidos a los que podemos acceder.

Los dispositivos, principalmente los *smartphones* o teléfonos inteligentes, nos permiten tener múltiples instrumentos en uno solo. Solo 10 años atrás, necesitábamos llevar con nosotros, además del teléfono celular para poder hablar, un aparato para escuchar música, una cámara para poder tomar fotografías, una agenda para ver el calendario, un cuaderno que nos permitiera tomar notas y escribir, un mapa para poder ubicarnos o un gps, entre otros ejemplos.

Con el desarrollo de los *smartphones* o teléfonos inteligentes, tenemos todas esas funciones mencionadas, y muchas otras, en un único dispositivo. Vale destacar que hasta hace relativamente pocos años, escasas personas podían acceder a este tipo de dispositivos, mas actualmente el uso es masivo. El cambio en el modo de consumo, gracias a la digitalización, impactó en múltiples industrias y solo aquellos que fueron capaces de ver el cambio y de transformarse pudieron seguir adelante. Un ejemplo muy conocido es el de Kodak, quien, si bien fue capaz de invertir en el cambio, no lo ejecutó a tiempo.

Tener todo centralizado en un único dispositivo, sumado a la conectividad y al desarrollo de plataformas electrónicas, tiene muchos beneficios, en tanto permite –entre otras cosas– que las personas se expresen con mayor facilidad y alcance, al tiempo que puedan consumir, generar y acceder a más contenidos.

Sin perjuicio, las personas tienen sus vidas cada vez más sumergidas en Internet, lo cual genera riesgos en lo que respecta a la protección de los datos personales y a su privacidad.

Con la digitalización de la información, es más simple generar, procesar, almacenar y transmitir contenido. Un buen uso de la información puede generar múltiples beneficios; mas es importante generar las condiciones para que se puedan utilizar los datos, sin vulnerar los derechos fundamentales de las personas.

Asimismo, con el desarrollo de servicios y aplicaciones digitales, principalmente a través de las diversas plataformas que se generan, tenemos la posibilidad de acceder a múltiples servicios, de calidad, de forma inmediata, y en algunos casos de manera gratuita.

En lo que respecta a las redes de infraestructura y a los servicios que se pueden brindar a través de las mismas, se debe considerar que con la convergencia cambian los modelos de negocios de los operadores de telecomunicaciones y la forma de amortizar la infraestructura.

En el modelo tradicional, cada red estaba habilitada para prestar un determinado servicio y se compensaba con la prestación del servicio que se brindaba sobre la misma. Por ejemplo: las inversiones que se debían hacer en la red del servicio de telefonía fija se atendían con los ingresos que se conseguían con la prestación de ese mismo servicio.

Actualmente esa lógica cambió, ahora se pueden prestar diversos servicios a través de una sola red, utilizando la misma infraestructura. Al mismo tiempo, los servicios tradicionales pasan a prestarse sobre una única red, a través del servicios de transmisión de datos o Internet, e ingresan nuevos jugadores, especializados, que con el desarrollo de plataformas electrónicas, fragmentan procesos y negocios, compitiendo y sustituyendo a los servicios tradicionales, pero sin tener que invertir en la infraestructura o en la red clásica.

Esto genera grandes desafíos, no solo porque se genera más competencia, integrando modelos verticales gracias a la interoperabilidad, sino que además, como indicamos, cambia el modelo de negocio, la red ya no se amortiza directamente con el servicio que se brinda sobre la misma, al tiempo que la red se utiliza cada vez más, demandando por ende más capacidad, velocidad y seguridad, para lo que se necesita despliegue e inversión en nuevas tecnologías.

Todos –personas, empresas, gobiernos, academia, etc.– tenemos el desafío de transformarnos digitalmente, lo cual implica que innovemos y que incorporemos la tecnología en los diversos procesos, simplificando, integrando y utilizando los datos de forma inteligente. Lo anterior se potencia aún más con el desarrollo de las tecnologías de avanzada, como ser la inteligencia artificial, la robótica, el Internet de las cosas, *big data*, almacenamiento en la nueva y *blockchain*; así como con el desarrollo de las redes de conectividad 5G y de alto rendimiento.

Ante este escenario, donde se borran las fronteras y la forma de prestar los servicios evoluciona constantemente, pudiendo prestarse por diversos medios; es esencial que se reconozca el principio de neutralidad tecnológica, así como que se

compartan eficientemente los recursos, como ser el espectro radioeléctrico, el espacio físico, el soporte de redes y las redes de acceso y transporte.

Al respecto, es interesante destacar que el Código Europeo de Comunicaciones Electrónicas reconoce: (i) que las capacidad de las redes de comunicaciones electrónicas están en constante aumento, (ii) que parámetros como la latencia, la disponibilidad y la fiabilidad toman cada vez mayor importancia, (iii) que el medio a través del cual se presta un servicio de conectividad va a ser cada vez menos importante, en tanto ofrezcan un rendimiento de red similar, (iv) que la neutralidad tecnológica solo debe aplicarse ante la necesidad de evitar interferencias perjudiciales, (v) que no se debería excluir la posibilidad de utilizar más de un servicio en la misma banda de espectro radioeléctrico, sino que los usuarios de los mismos deberían poder elegir las tecnologías y los servicios, a menos que estén en juego objetivos de interés general, debidamente justificado y revisados periódicamente[80].

Como reflejo de lo anterior, los servicios tradicionales de telecomunicaciones pierden público constantemente, no es porque los mismos se dejen de demandar, sino que ahora se utilizan de manera diferente, sobre Internet.

Por ejemplo, en el mundo el uso de la telefonía fija marca una tendencia negativa desde hace varios años, mientras que la telefonía móviles marca una tendencia positiva, sin embargo, el crecimiento se desaceleró, y en algunos países, como España, el uso descendió[81].

En el caso de Uruguay, interesa destacar que como surge del Informe "Evolución del sector telecomunicaciones en Uruguay"[82], realizado por la Unidad Reguladora de Servicios de Comunicaciones (URSEC), a junio de 2018, si comparamos el primer semestre de 2013 con el primer semestre de 2018, en los últimos 5 años vemos que: (i) la cantidad de mensajes de textos enviados cayó más de un 80 %; (ii) la cantidad de

80 Exposición de motivos del Código Europeo de Comunicaciones Electrónicas. URL: https://eur-lex.europa.eu/legal-content/ES/ALL/?uri=CELEX:52016PC0590 Consultado el 9 de febrero de 3029.

81 ONTSI, Informe Anual "La Sociedad en Red" Edición 2018. URL: https://www.ontsi.red.es/sites/ontsi/files/La%20sociedad%20en%20red.%20Informe%20anual%202017%20(Edici%c3%b3n%202018).pdf Consultado el 1 de junio de 2019.

82 Unidad Reguladora de Servicios de Comunicaciones, Informe de Mercado Telecomunicaciones, Junio 2018. URL: https://www.ursec.gub.uy/inicio/transparencia/informacion-estadistica-y-de-mercado/telecomunicaciones/ Consultado el 9 de febrero de 2019.

minutos de tráfico del servicio de larga distancia internacional salientes cayó más del 50 %; (iii) la cantidad de minutos de voz de servicios móviles cayó casi un 25 %.

Los cambios señalados, en especial las caídas que están experimentando algunos servicios no sorprenden, cada vez es más extraño que utilicemos el servicio de telefonía fija, que enviemos mensajes de texto tradicionales, que llamemos al exterior por el servicio de larga distancia internacional o que llamemos por el servicio móvil tradicional. Lo anterior no es porque hablemos menos por teléfono o porque enviemos menos mensajes que antes, sino que lo hacemos de manera diferente, ahora utilizamos plataformas electrónicas, como pueden ser: WhatsApp, Facebook, Skype, Telegram, etc., que se enfocan en servicios específicos, innovan en relación al servicio tradicional, prestando el mismo servicio pero a través de medios diversos, generando muchos beneficios para los usuarios.

En línea con lo anterior, como surge del Informe de URSEC antes referenciado, en el primer semestre del año 2018, el tráfico de datos de servicios móviles subió un 7 %. Como indicábamos, cambia el modelo.

Actualmente, hay un servicio, transmisión de datos e Internet, que habilita a terceros a ofrecer sobre ese único servicio, diversos contenidos que compiten directamente y sustituyen los servicios tradicionales. Estamos en un escenario nuevo, que necesariamente requiere que se revise la regulación tradicional, se debe tener en cuenta a todo el ecosistema digital y no se debe regular por la tecnología.[83]

En este contexto, el principio de neutralidad tecnológica, así como la coordinación y compartición de recursos toman mayor relevancia. Internet está presente en todo, permitiendo que diversas actividades se puedan brindar sobre la red. Al usuario final le es indiferente si el proveedor transporta directamente la señal o si lo hace a través de un servicio de acceso a Internet, siempre que la calidad sea similar.[84]

En definitiva, se presentan cambios económicos y sociales de gran magnitud, que implican grandes beneficios para todos, al tiempo que generan riesgos para los derechos fundamentales y para la economía tradicional. Se debe buscar que los derechos

83 BELLO, PABLO Y SASTRE, ANDRÉS, "Re-pensar las políticas públicas para el cierre de la brecha digital en América Latina" en *Gobernanza y regulaciones de Internet en América Latina. Análisis en honor a los diez años de la South School on Internet Governance*, FGV Direito Rio, Río de Janeiro, 2018, pp. 250 y ss.

84 Código Europeo de Comunicaciones Electrónica.

fundamentales se respetan tanto *online* como *offline*, y que no se generen ventajas competitivas a consecuencia de asimetrías regulatorias, se debe buscar que los mismos servicios, independientemente del medio a través del cual se brinden, tengan las mismas regulaciones.

La forma no es prohibir o establecer regulaciones sin sentido, porque de esa forma se afecta al usuario, así como al desarrollo social y económico de todos; sino que lo que tenemos que hacer es repensar los modelos.

Tenemos que darle la bienvenida a la innovación, pero no podemos celebrar asimetrías regulatorias ante supuestos similares. Las formas cambian, los modelos de negocio también, y sin duda, en muchos casos la regulación vigente no refleja la realidad. Todo lo anterior hace necesario un análisis cabal de la regulación, buscando que la misma responda a la realidad, poniendo a las personas en el centro, permitiendo el desarrollo económico y social de todos.

V. Gobernanza

Como surge de las diversas agendas digitales –tanto regionales, como nacionales–, la infraestructura, especialmente la vinculada a las redes de telecomunicaciones, es la base sobre la cual se construye y desarrolla el mundo digital.

La Unión Europea compara a la banda ancha con el oxígeno para todos, destacando que el desarrollo de redes de alta velocidad tiene el mismo impacto hoy que en el siglo pasado tuvieron las redes eléctrica y de transporte. Las redes de telecomunicaciones de última generación son de suma importancia para que la digitalización se pueda universalizar debidamente y para que todos podamos gozar de los beneficios que la revolución digital ofrece.

No cabe duda que, como lo indica el preámbulo de la Ley General de Telecomunicaciones de España, N° 9/2014[85], *"Las telecomunicaciones constituyen uno de los sectores más dinámicos de la economía y uno de los que más pueden contribuir al crecimiento, la productividad, el empleo, y por tanto, al desarrollo económico y al bienestar social, afectando directamente al círculo de protección de los intereses generales.*

85 https://www.boe.es/buscar/act.php?id=BOE-A-2014-4950 Consultado el 15 de enero de 2020.

Actualmente, la evolución tecnológica nos sitúa en una nueva etapa –la de extensión de las redes de nueva generación–, que obliga a los poderes públicos a reflexionar sobre la importancia de la función regulatoria.

La situación económica y financiera que afecta a una gran parte de los países desarrollados, la necesidad actual de fomentar la inversión e impulsar la competencia, son elementos esenciales a considerar en la revisión del marco regulador.

El sector de las telecomunicaciones, sujeto a un proceso de permanente innovación tecnológica, necesita de constantes e ingentes inversiones, lo que requiere acometer proyectos de gran envergadura que pueden verse afectados si se exigieran en condiciones distintas de despliegue de redes y de comercialización de servicios en los diferentes ámbitos territoriales."

Las telecomunicaciones son esenciales para poder alcanzar los objetivos planteados en las Agendas Digitales y tienen un rol fundamental en la transformación digital. El despliegue de infraestructura es clave y requiere de la coordinación de múltiples factores para generar las condiciones adecuadas para que las redes y los servicios innovadores prosperen. Para esto, entre otros aspectos, es esencial que la normativa sea adecuada, que otorgue seguridad y previsibilidad, que se pueda coordinar la asignación del espectro, compartir los recursos y crear incentivos para la inversión en redes de última tecnologías, generando un marco institucional eficaz.

En esta línea, vale destacar los tres pilares de la posición tomada por Estados Unidos en el año 2003, manifestada por David Gross: (1) enfatizar el Estado de Derecho para atraer inversiones necesaria para la infraestructura, (2) crear contenidos y proteger la propiedad intelectual, y (3) garantizar la seguridad en Internet, en las comunicaciones y en el comercio electrónico[86].

Asimismo, es interesante como lo manifiesta Raúl Echeberría[87] "*En todo el mundo podemos ver intensos debates, entre otros temas, sobre el impacto de la economía digital en las economías locales, el impacto de la inteligencia artificial en el mercado laboral, cómo aplicar los existentes marcos tributarios a los nuevos modelos*

[86] https://es.qaz.wiki/wiki/World_Summit_on_the_Information_Society Consultado el 8 de diciembre de 2020.

87 ECHEBERRÍA, RAÚL, "Construyendo modelos innovadores de gobernanza" en *Gobernanza y Regulaciones de Internet en América Latina. Análisis en honor a los diez años de la South School on Internet Governance*, FGV Direito Rio, Río de Janeiro, 2018, pp. 12 y ss.

de negocios, los desafíos de la ciberseguridad, el efecto de las noticias falsas, la seguridad de Internet de las cosas, o la posibilidad del uso de armas cibernéticas en distintos tipos de conflictos.

Estos son solo algunas de las discusiones que vemos emerger en distintos ámbitos a nivel global.

Tanto las necesidades de incrementar el acceso a Internet como estos otros temas emergentes, configuran nuevos desafíos que no pueden ser resueltos con las mismas herramientas políticas y a través de los mismos mecanismos con los que enfrentábamos problemas pasados.

Nuevos desafíos demandan nuevos enfoques, enfoques que sean innovadores tanto desde el punto de vista de los contenidos como desde las formas".

Sin duda la nueva realidad digital presenta múltiples retos para la regulación, tanto en lo que respecta a los contenidos, como en lo relacionado a la jurisdicción. Sin perjuicio, lo esencial es construir un sector sostenible, que capte inversiones para el desarrollo de infraestructuras, que cree contenido, que respete los derechos fundamentales de las personas y los principios generales de derechos, y que otorgue seguridad para innovar continuamente.

Hay diversas posiciones o tesis en lo que respecta a la posibilidad de regular las acciones de las personas en el ámbito digital[88].

Por un lado tenemos a quienes declaran la independencia del ciberespacio, realizada por John Perry Barlow en 1996. Se basa en la libertad en el ciberespacio, como un sitio independiente, diferente, en el que los gobiernos tradicionales no pueden imponer sus leyes, su jurisdicción.

Ante estas posiciones, surgen reacciones como la del Profesor Chris Reed que llamó al ciberliberalismo una falacia, destacando que todos los actores involucrados en una transacción en Internet tienen una existencia en el mundo real, están ubicados en algún sitio, en una jurisdicción, por lo que no tiene sentido que no se puedan aplicar las leyes.

88 MURRAY, ANDREW, obra citada, ps. 60 y ss.

Por otra parte, tenemos al ciberpaternalismo, donde se destaca la figura de Joel Heidelberg, de Fordham Law School, quien sostiene que nuevos modelos y fuentes de normas se están creando e identifica dos limites, involucrando a los estados, al sector privado, el interés técnico y a los ciudadanos. El primer límite está establecido en los acuerdos contractuales que se celebren, y el segundo límite se encuentra en la arquitectura de la red, que fue realizada por el hombre, por lo que está bajo su control. Considera que quienes diseñan las normas pueden establecer controles a las actividades y a las personas en el mundo *online,* indirectamente, disponiendo cambios en la arquitectura de las redes o estableciendo actividades de auto regulación en el diseño de las redes.

El profesor Lawrence Lessig desarrolló la idea de Reidenberg en su texto "Code and Other Laws of Cyberspace". Entendía que había cuatro formas de regular, que comprendían las formas de actuar de los individuos, las cuales se podían usar de forma individual o híbrida, directa o indirectamente, por los reguladores para controlar la actividad de los individuos en el mundo *online* u *offline*. Estos factores eran: (1) las leyes, por la amenaza de una penalización, (2) las normas sociales, que pueden derivar en sanciones sociales como ser criticado, (3) el mercado, que depende de la competencia y de los precios, y (4) la arquitectura física, por ejemplo a través del bloqueo.

Una tercera forma de pensamiento es la del "comunitarismo", impulsada por Murray en su obra "*The Regulation of Cyberspace: Control in the online Environment",* la cual se distingue de las dos tendencias anteriores, reparando en una relación entre el entorno digital y el real, entendiendo que la regulación es un proceso de diálogo entre los individuos y la sociedad. Partiendo de la teoría de Lessig, toma las leyes, las normas sociales y el mercado, y concibe que hay una aproximación por el control, teniendo como base la comunidad. Por ejemplo: (i) las leyes son aprobadas por quienes dictan las normas que son elegidos por la comunidad; (ii) el mercado es un reflejo de los valores, de la demanda, de las provisiones, reflejando a la comunidad en términos monetarios; y (iii) las normas sociales, son una codificación de los valores comunitarios. En este sentido, se diferencia de Lessig en que encuentra que hay que reemplazar los puntos aislados por una red comunitaria de puntos que comparten ideas, pensamientos, opiniones, etc., y en que considera que el proceso regulatorio es en realidad un diálogo natural, no una externalidad.

Una cuarta forma de regular es a través de la regulación privada o autorregulación. Un ejemplo es a través de lo que se establece en los términos y condiciones de los contratos de los servicios brindados por los diversos proveedores. Otro ejemplo, son los acuerdos que se realizan entre la propia industria, como se hizo en Inglaterra para prevenir el acceso a contenidos ilegales, como ser el acceso a imágenes de menores abusados. En este caso, se hizo una alianza entre los proveedores de servicios y la organización "Internet Watch Foundation" (iwf) para bloquear el acceso a dichos contenidos. Este requerimiento se implementó por los operadores, sin que se necesitara legislación. Un ejemplo similar se puede señalar en Uruguay, en tanto se celebró un Acuerdo de Intercambio de Listas Negativas, entre los proveedores de servicios móviles en el año 2011. Los operadores acordaron, por sí, sin que hubiera una obligación legal en ese momento, que intercambiarían a diario las listas de los celulares que se denunciaran como robados, obligándose a bloquearlos en sus redes, como forma de desestimular el hurto de los equipos.

La quinta forma de regular implica la regulación supranacional. Se destaca: (i) la Unión Internacional de Telecomunicaciones (uit o itu por sus siglas en inglés)), (ii) la Cumbre sobre la Sociedad de la Información (cmsi), (iii) los Foros de Gobernanza de Internet (fgi) y (iv) a nivel de la Unión Europea, las Directivas o Reglamentaciones que se dicten.

Procedemos a comentar sobre este último aspecto, específicamente los ejemplos de regulación supranacional mencionados.

(V.1.) La Unión Internacional de Telecomunicaciones

Como indicáramos en otras ocasiones[89], la UIT es el organismo de las Naciones Unidas para las Tecnologías de la Información y la Comunicación - TIC[90], cuenta con 193 países miembros y más de 700 entidades del sector privado e instituciones académicas. Los miembros tienen los derechos y están sujetos a las obligaciones previstas en la Constitución y en el Convenio de la uit.

El Convenio y la Constitución de la UIT son los instrumentos fundamentales de la Unión, los cuales se complementan con Reglamentos Administrativos, como ser el

89 Véase nuestro trabajo en ARAMENDÍA, MERCEDES, "Aspectos fundamentales de los servicios de telecomunicaciones en el país" en *Estudios de Telecomunicaciones y Sociedad de la Información,* Universidad de Montevideo, 2018, pp. 55 y ss.

90 https://www.itu.int/es/about/Pages/default.aspx Consultado el 5 de febrero de 2018.

Reglamento de las Telecomunicaciones Internacionales y el Reglamento de Radiocomunicaciones, que regulan el uso de las telecomunicaciones, tienen carácter vinculante para todos los Miembros, prevaleciendo en caso de divergencia siempre la Constitución y luego el Convenio.

Como surge del Preámbulo de la Constitución de la UIT,se reconoce en toda su plenitud el derecho soberano de cada Estado a reglamentar sus telecomunicaciones, así como la importancia creciente que tienen las telecomunicaciones para la salvaguardia de la paz y para el desarrollo económico y social de todos los Estados. El fin de la Constitución y del Convenio de la UIT es facilitar las relaciones pacíficas, la cooperación internacional entre los pueblos y el desarrollo económico y social por medio del buen funcionamiento de las telecomunicaciones.

Los Miembros están obligados a atenerse a las disposiciones de la Constitución, del Convenio y de los Reglamentos Administrativos en todas las oficinas y estaciones de telecomunicaciones instaladas o explotadas por ellos y que presten servicios internacionales o puedan causar interferencias perjudiciales a los servicios de radiocomunicación de otros países, excepto en lo relativo a las instalaciones radioeléctricas militares conforme el Artículo 37 de la Constitución de la uit. Además, los Miembros deben adoptar las medidas necesarias para imponer observancia de las disposiciones de los instrumentos de la Unión a las empresas de explotación por ellos autorizadas, para establecer y explotar telecomunicaciones y que presten servicios internacionales o que exploten estaciones que puedan causar interferencias perjudiciales a los servicios de radiocomunicación de otros países.[91]

La Unión tiene por objeto, entre otras cosas: (a) mantener y ampliar la cooperación internacional entre los miembros para el mejoramiento y el empleo racional de toda clase de telecomunicaciones, así como promover y proporcionar asistencia técnica a los países en desarrollo en el campo de las telecomunicaciones; (b) impulsar el desarrollo de los medios técnicos y su más eficaz explotación, a fin de aumentar el rendimiento de los servicios de telecomunicaciones, acrecentar su empleo y generalizar lo más posible su utilización por el público; (c) promover la utilización de los servicios de telecomunicaciones con el fin de facilitar las relaciones pacíficas; y (d) armonizar los esfuerzos de los Miembros para consecución de estos fines.

91 Artículo 6 de la Constitución de la UIT.

A estos efectos, la UIT, entre otras cosas[92]:

a. *efectuará la atribución de las bandas de frecuencias del espectro radioeléctrico, la adjudicación de frecuencias radioeléctricas y llevará el registro de las asignaciones de frecuencias y las posiciones orbitales asociadas en la órbita de los satélites geoestacionarios, a fin de evitar toda interferencia perjudicial entre las estaciones de radiocomunicaciones de los distintos países;*

b. *coordinará los esfuerzos para eliminar las interferencias perjudiciales entre las estaciones de radiocomunicaciones de los diferentes países y para mejorar la utilización del espectro de frecuencias radioeléctricas y de la órbita de los satélites geoestacionarios para los servicios de radiocomunicación;*

c. *facilitará la normalización mundial de las telecomunicaciones con una calidad de servicio satisfactoria;*

d. *fomentará la cooperación internacional en el suministro de asistencia técnica a los países en desarrollo, así como la creación, el desarrollo y el perfeccionamiento de las instalaciones y de las redes de telecomunicación en los países en desarrollo por todos los medios de que dispongan, y en particular, por medio de su participación en los programas adecuados de las Naciones Unidas y el empleo de sus propios recursos, según proceda;*

e. *coordinará siempre los esfuerzos por armonizar el desarrollo de los medios de telecomunicación, especialmente los que utilizan técnicas especiales, a fin de aprovechar al máximo sus posibilidades;*

f.*fomentará la colaboración entre los Miembros con el fin de llegar, en el establecimiento de tarifas, al nivel mínimo compatible con un servicio de buena calidad y con una gestión financiera de las telecomunicaciones sana e independiente;*

g. *promoverá la adopción de medidas destinadas a garantizar la seguridad de la vida humana, mediante la cooperación de los servicios de telecomunicación;*

h. *emprenderá estudios, establecerá reglamentos, adoptará resoluciones, formulará recomendaciones y ruegos, reunirá y publicará información sobre las telecomunicaciones;*

92 Artículo 1.2 de la Constitución de la UIT.

i.*promoverá, ante los organismos financieros internacionales, el establecimiento de líneas de crédito preferenciales y favorables con miras al desarrollo de proyectos sociales orientados a extender los servicios de telecomunicaciones a las zonas más aisladas de los países.*

La UIT está compuesta por los siguientes órganos[93]:

1. La Conferencia de Plenipotenciarios: órgano supremo de la Unión. Constituida por delegaciones que representan a los Miembros y se convoca normalmente cada cinco años, en todo caso el intervalo entre una conferencia y otra no puede exceder los seis años. Entre sus cometidos se destaca el determinar los principios generales aplicables para alcanzar el objeto de la UIT,fijar las bases del presupuesto de la Unión, determinar el tope de sus gastos, dar instrucciones generales relacionadas con la plantilla de personal de la UIT,aprobar las cuentas de la Unión, elegir a los Miembros que han de constituir el Consejo de Administración, elegir al Secretario General y Vicesecretario General, elegir a los Miembros de la Junta Internacional de Registro de Frecuencias, elegir a los miembros de los Comités Consultivos Internacionales, elegir al Director de la Oficina de Desarrollo de las Telecomunicaciones, aprobar las enmiendas a la Constitución y al Convenio, revisar los acuerdos y tratar todos los asuntos de telecomunicaciones que juzgue necesario.

2. Las conferencias administrativas: comprende las mundiales y las regionales. Normalmente son convocadas para estudiar cuestiones particulares de telecomunicaciones y se limitan estrictamente a tratar asuntos que figuren en su orden del día. El orden del día podrá incluir temas vinculados a los Reglamentos Administrativos y puntos relativos a cuestiones específicas de telecomunicaciones de carácter regional.

3. El Consejo de Administración: el número de miembros de la Unión será determinado por la Conferencia de Plenipotenciarios, este número no excederá el 25 % del número total de Miembros de la Unión. El Consejo establecerá su propio Reglamento interno, en el intervalo de la Conferencia de Plenipotenciarios, actuará como mandatario de dicha conferencia, dentro de los límites de las facultades que le delegue. Entre sus cometidos se encuentran los siguientes: adoptar medidas para facilitar la aplicación por los Miembros de las disposiciones de los instrumentos de la

93 Artículo 7 de la Constitución de la UIT.

UIT,determinar anualmente la política de asistencia técnica conforme al objeto de la Unión, coordinar la actividad de la Unión, ejercer un control financiero efectivo sobre sus órganos permanentes, y promover la cooperación internacional para proporcionar cooperación técnica a los países en desarrollo por todos los medios de que disponga.

4. Los órganos permanentes que a continuación se enumeran:

i. la Secretaría General: dirigida por un Secretario General, auxiliado por un Vicesecretario General, que actuará como representante de la Unión. Tomarán posesión de sus cargos en las fechas que se determinen en el momento de su elección, permanecerán en funciones hasta la fecha que determine la siguiente Conferencia de Plenipotenciarios y sólo serán reelegibles una vez. Tomará las medidas necesarias para garantizar la utilización económica de los recursos de la Unión y responderá ante el Consejo de Administración de todos los aspectos administrativos y financieros de las actividades.

ii. La Junta Internacional de Registro de Frecuencias (ifrb): estará integrada por cinco miembros independientes elegidos por la Conferencia de Plenipotenciarios entre los candidatos propuestos por los Miembros de la Unión de manera que quede garantizada una distribución equitativa entre las regiones del mundo. Cada miembro solo podrá proponer un candidato, que será uno de sus nacionales, tomarán posesión en las fechas que se fijen en el momento de su elección, permanecerán en funciones hasta la fecha que determine la Conferencia de Plenipotenciarios siguiente y serán reelegibles una sola vez. En el desempeño de su cometido, los miembros de la Junta Internacional de Registro de Frecuencias no actuarán en representación de sus respectivos Estados Miembros ni de una región determinada, sino como depositarios de la fe pública internacional.

Entre las funciones esenciales tiene las siguientes: (a) efectuar la inscripción y registro metódico de las asignaciones de frecuencias notificadas por los diferentes Miembros, con las decisiones de las conferencias competentes de la Unión, con el fin de garantizar su reconocimiento internacional oficial; (b) efectuar en las mismas condiciones y con el mismo objeto la inscripción metódica de las frecuencias y posiciones orbitales asociadas asignadas por los Miembros a los satélites geoestacionarios; (c) asesorar a los Miembros para la explotación del mayor número posible de canales radioeléctricos en las regiones del espectro de frecuencias en que puedan producirse interferencias perjudiciales y la utilización equitativa, eficaz y

económica de la órbita de los satélites geoestacionarios; (d) llevar a cabo las demás funciones complementarias, relacionadas con la asignación y utilización de las frecuencias y con la utilización equitativa de la órbita de los satélites geoestacionarios, conforme a los procedimientos previstos en el Reglamento de Radiocomunicaciones; (e) prestar asistencia técnica para la preparación de las conferencias de radiocomunicaciones consultando, si procede, a los otros órganos competentes de la Unión; (f) tener al día los registros indispensables para el cumplimiento de sus funciones; y (g) intercambiar, cuando proceda, con los Miembros de la Unión datos de la Junta Internacional de Registro de Frecuencias.

iii. El Comité Consultivo Internacional de Radiocomunicaciones (ccir): realiza estudios sobre las cuestiones técnicas y de explotación relativas específicamente a las radiocomunicaciones sin limitación de la gama de frecuencias y formula recomendaciones al respecto para la normalización de las telecomunicaciones a escala mundial.

iv. El Comité Consultivo Internacional de Telegráfico y Telefónico (ccitt): estudia las cuestiones técnicas, de explotación y de tarificación relacionadas con las telecomunicaciones y formula recomendaciones al respecto para la normalización de las telecomunicaciones a escala mundial salvo las cuestiones técnicas y de explotación que se refieren específicamente a las radiocomunicaciones que competen al Comité Consultivo Internacional de Radiocomunicaciones.

En el cumplimiento de sus misiones, el ccir y el ccitt prestan la debida atención al estudio de los problemas y a la elaboración de las recomendaciones directamente relacionadas con la creación, el desarrollo y el perfeccionamiento de las telecomunicaciones en los países en desarrollo, en los planos regional e internacional. Son miembros: por derecho propio, las administraciones de los Miembros de la Unión, las empresas privadas de explotación reconocidas y organizaciones científicas o industriales que, con la aprobación del Miembro Correspondiente, manifiesten el deseo de participar en los trabajos de estos Comités.

Cada Comité cumplirá sus tareas mediante: la Asamblea Plenaria, las comisiones de estudio que instituya, y por un director, elegido por la Conferencia de Plenipotenciarios para el período comprendido entre dos Conferencias de Plenipotenciarios. Será reelegible una sola vez.

v. La Oficina de Desarrollo de las Telecomunicaciones (bdt): sus funciones consisten en cumplir con el objeto de la Unión en el marco de su esfera de competencia específica, el doble cometido de la Unión como organismo especializado de las Naciones Unidas y como organismo ejecutor para la realización de proyectos de desarrollo del sistema de las Naciones Unidas y de otras iniciativas de financiación, con objeto de facilitar y potenciar el desarrollo de las telecomunicaciones ofreciendo, organizando y coordinando actividades de cooperación y asistencia técnica.

En este contexto, la bdt tiene entre sus funciones: (a) crear una mayor conciencia en los responsables de decisiones acerca del importante papel que desempeñan las telecomunicaciones en los programas nacionales de desarrollo socioeconómico, y facilitar información y asesoramiento sobre posibles opciones de política; (b) promover el desarrollo, la expansión y la explotación de las redes y servicios de telecomunicaciones, particularmente en los países en desarrollo, teniendo en cuenta las actividades de otros órganos pertinentes, y reforzando las capacidades de revalorización de recursos humanos, planificación, gestión, movilización de recursos, investigación y desarrollo; (c) potenciar el crecimiento de las telecomunicaciones mediante la cooperación con organizaciones regionales y con instituciones de financiación del desarrollo mundial y regional; (d) alentar la participación de la industria al desarrollo de las telecomunicaciones en los países en desarrollo, ofrecer asesoramiento sobre la elección y la transferencia de la tecnología apropiada; (e) ofrecer asesoramiento y realizar o patrocinar, en su caso, los estudios necesarios sobre cuestiones técnicas, económicas, financieras, administrativas, reglamentarias y de política general, incluido el estudio de proyectos concretos en el campo de las telecomunicaciones; (f) colaborar con los Comités Consultivos Internacionales y otros órganos interesados, en la preparación de un plan general de redes de telecomunicaciones internacionales y regionales, con objeto de facilitar el desarrollo coordinado de las mismas para ofrecer servicios; (g) proporcionar apoyo para la preparación y organización de conferencias de desarrollo.

La bdt cumplirá sus tareas mediante conferencias mundiales y conferencias regionales de desarrollo, y por un director, elegido por la Conferencia de Plenipotenciarios para el período comprendido entre dos Conferencias de Plenipotenciarios, será reelegible sólo una vez.

Por otra parte, hay un Comité de Coordinación que está constituido por el Secretario General, el Vicepresidente General, los Directores de los Comités Consultivos internacionales, el Director de la Oficina de Desarrollo de las Telecomunicaciones y el Presidente y el Vicepresidente de la Junta Internacional de Registro de Frecuencias. Su Presidente es el Secretario General, y en su ausencia el Vicesecretario General. El Comité asesora y auxilia al Secretario General en todo los asuntos administrativos, financieros y de cooperación técnica que afecten a más de un órgano permanente, así como en lo que respecta a las relaciones exteriores y a la información pública.

Vale indicar que la Constitución establece disposiciones generales relativas a las telecomunicaciones, entre ellas se destacan:

a. El reconocimiento al público del derecho a comunicarse por medio del servicio internacional de correspondencia pública, siendo los servicios, las tasas y las garantías las mismas, en cada categoría de correspondencia, para todos los usuarios, sin prioridad ni preferencia alguna.

b. La reserva al derecho a detener todo telegrama privado que pueda parecer peligroso para la seguridad del Estado o contrario a sus leyes, al orden público o a las buenas costumbres, a condición de notificar inmediatamente a la oficina de origen la detención, a no ser que la notificación se juzgue peligrosa para la seguridad del Estado, así como la reserva al derecho a interrumpir otras telecomunicaciones privadas que puedan parecer peligrosas para la seguridad del Estado o contrarias a sus leyes, al orden público o a las buenas costumbres.

c. El compromiso a adoptar todas las medidas que permitan los sistemas para garantizar el secreto de la correspondencia internacional, reservando el derecho a comunicar esta correspondencia a las autoridades competentes, con el fin de garantizar la aplicación de su legislación nacional o la ejecución de los convenios internacionales que sean parte.

d. La reserva del derecho a suspender el servicio de telecomunicaciones internacionales, bien en su totalidad o solamente para ciertas relaciones y para determinadas clases de correspondencia de salida, llegada o tránsito, con la obligación de comunicarlo inmediatamente, por conducto del Secretario General, a los demás miembros.

e. Adoptar las medidas procedentes para el establecimiento, en las mejores condiciones técnicas, de los canales o instalaciones necesarios para el intercambio rápido e ininterrumpido de las telecomunicaciones internacionales.

f.Dar prioridad absoluta a todas las telecomunicaciones relativas a la seguridad de la vida humana en el mar, en tierra, en el aire y en el espacio ultraterrestre, así como a las telecomunicaciones epidemiológicas de urgencia excepcional de la Organización Mundial de la Salud.

g. Procurar limitar las frecuencias y el espectro utilizado al mínimo indispensable para obtener el funcionamiento satisfactorio de los servicios necesarios. A tal fin, se esforzarán por aplicar, a la mayor brevedad, los últimos adelantos de la técnica. Al respecto, en la utilización de bandas de frecuencias para las radiocomunicaciones, los Miembros tendrán en cuenta que las frecuencias y la órbita de los satélites geoestacionarios son recursos naturales limitados que deben utilizarse de forma racional, eficaz y económica, de conformidad con lo establecido en el Reglamento de Radiocomunicaciones.

h. Todas las estaciones deberán ser instaladas y explotadas de tal manera que no puedan causar interferencias perjudiciales a las comunicaciones o servicios radioeléctricos de otros Miembro, de las empresas privadas de explotación reconocidas o de aquellas otras debidamente autorizadas para realizar un servicio de radiocomunicación y que funcionen de conformidad con las disposiciones del Reglamento de Radiocomunicaciones.

(V.2.) Cumbre Mundial sobre la Sociedad de la Información (CMSI)

En 1998 la Conferencia de Plenipotenciarios de la UIT dictó la Resolución 73, relativa a la cmsi, observando que las telecomunicaciones desempeñan cada vez más un rol determinante en los planos político, económico, social y cultural, reconocen que la UIT es la organización más apta para buscar las formas para alcanzar el desarrollo del sector de las telecomunicaciones, complementando su acción con las de otras organizaciones internacionales y regionales.

Considerando el carácter mundial de las telecomunicaciones y de la importancia que tienen para el desarrollo de la sociedad de la información, son conscientes de la necesidad de fomentar una evolución armoniosa de las políticas, de las

reglamentaciones, de los servicios y de las redes en todos los Estados Miembros; por lo que encargan: (i) al Secretario General la celebración de una cmsi, y (ii) al Consejo que examine y determine la contribución de la Unión a la organización de dicha cumbre a fin de: (a) establecer un concepto común y armonizado de la sociedad de la información, (b) elaborar un plan de acción estratégico para el desarrollo de la sociedad de la información, y (c) determinar las funciones de los diferentes asociados.

Partiendo de esa base, se hizo una primer fase en Ginebra y una segunda fase en Túnez.

La primer fase tuvo lugar en diciembre de 2003, se buscaba una declaración de voluntad política, y tomar medidas concretas para preparar los fundamentos de la Sociedad de la Información. Finalizó con la aprobación de la Declaración de Principios y de un Plan de Acción[94].

La Declaración de Principios de Ginebra se aprobó en mayo del 2004, en vistas de construir una Sociedad de la Información centrada en la persona, integradora y orientada al desarrollo, sobre la base de la Carta de las Naciones Unidas y respetando la Declaración Universal de Derechos Humanos.

Los principios parten de la base de que se quiere que las oportunidades que ofrecen las TIC alcancen y beneficien a todos; para lo cual se establecen los siguientes principios fundamentales:

1. Desarrollar y promover las TIC, para lo cual se debe cooperar y asociar a los gobiernos y a todos los interesados –sector privado, sociedad civil, Naciones Unidas y otras organizaciones–.

2. Promover el acceso universal a la conectividad, a la energía y a los servicios postales, para lo cual se requiere de infraestructura, banda ancha y otras tecnologías innovadoras, para acelerar el progreso económico y social de los países, así como el bienestar de las personas.

3. Acceder a la información y al conocimiento, así como contribuir con esa información, con ideas y conocimiento, lo cual es esencial en una Sociedad de la Información integradora.

94 Cumbre Mundial Sobre la Sociedad de la Información, URL: https://www.itu.int/net/wsis/geneva/index-es.html Consultado el 10 de febrero de 2019.

4. Crear las capacidades para que se adquieran las competencias y los conocimientos necesarios para comprender y participar en la Sociedad de la Información y en la economía del conocimiento.

5. Fomentar la confianza y la seguridad en la utilización de las TIC, desarrollar una cultura global de ciberseguridad, garantizar la protección de los datos y la privacidad, al tiempo que ampliar el acceso y el comercio.

6. Entorno nacional e internacional propicio, utilizando las TIC como una herramienta de buen gobierno. El derecho, acompañado de un marco político y reglamentario adecuado, transparente, favorable a la competencia, tecnológicamente neutro, predecible y que refleje la realidad.

7. Suministrar y aplicar los servicios TIC en beneficio de la población, ya sea para las actividades y servicios gubernamentales, para la atención y la información sanitaria, la educación, la capacitación, el empleo, la actividad económica, agropecuaria, el transporte, el medio ambiente, la vida cultural, para erradicar la pobreza, así como para otros objetivos de desarrollo.

8. Crear, difundir y preservar contenido en varios idiomas, prestando atención a la diversidad, a la identidad cultural, lingüística, al contenido local, así como al debido reconocimiento de los derechos de los autores y artistas.

9. Libertad de prensa y libertad de la información, independencia, pluralismo y diversidad de los medios de comunicación.

10. Respetar la paz y regirse por los valores fundamentales de libertad, igualdad, solidaridad, tolerancia, responsabilidad compartida y respeto a la naturaleza.

11. Cooperar a nivel internacional y regional entre los gobiernos, el sector privado, la sociedad civil y demás partes interesadas, entre ellas, las instituciones financieras internacionales.

El plan de acción se estableció en mayo de 2004, buscando ayudar a los países a superar la brecha digital, alcanzando la Sociedad de la Información de forma cooperativa y solidaria con los gobiernos y las demás partes interesadas.

La segunda fase de la cmsi se realizó en noviembre de 2005, en Túnez. Como consecuencia, en junio de 2006 se celebró el Compromiso de Túnez, reafirmando la

Declaración de Principios y el Plan de Acción de Ginebra, y se aprobó la Agenda de Túnez para la Sociedad de la Información.

Se partió de la base de que es necesario pasar a la acción, centrándose y haciendo hincapié en los mecanismos financieros destinados a colmar la brecha digital, en la gobernanza de Internet y en cuestiones afines, como el seguimiento y la implementación de las decisiones; si bien se reconoce la importancia y la responsabilidad de todas las partes, se destaca el rol fundamental de los gobiernos.

Diez años después, se celebró cmsi+10, donde se reconoció –entre otros aspectos– la necesidad de proteger y de reforzar todos los derechos humanos, su importancia para el desarrollo socioeconómico, así como la necesidad de garantizar que los derechos humanos prevalezcan y se respeten de igual manera en línea, como fuera de línea. Asimismo, se reafirmó que el Plan de Acción de Ginebra es una plataforma dinámica para promover la Sociedad de la Información en los planos nacionales, regionales e internacionales, se mejoraron las líneas de acción, y en lo que respecta al futuro, se dispuso: (i) que es esencial una cooperación efectiva entre los gobiernos, el sector privado, la sociedad civil, las Naciones Unidas y otras organizaciones internacionales, teniendo en cuenta el carácter multifacético de la creación de la Sociedad de la Información; (ii) que es importante la coordinación, para evitar la duplicación de actividades, intercambiar información, crear conocimientos, divulgar prácticas idóneas y ayudar en la concertación de asociaciones multipartitas y público-privadas; (iii) que el Grupo de las Naciones Unidas sobre la Sociedad de la Información (ungis) es esencial para coordinar las cuestiones de fondo y de política;. (iv) que se acoge con beneplácito la celebración anual del Foro de la cmsi, fundamental para el debate multipartito; (v) que se alienta a todos los interesados a aportar contribuciones y a colaborar; y (vi) que los compromisos para avanzar en la igualdad de género, deberían ser implementados, examinados y supervisados por onu Mujeres en cooperación con otras Líneas de Acción.

(V.3.) Foro de Gobernanza de Internet (FGI o IGF)

En el punto 72 de la Agenda de Túnez[95] se dispuso que se convocara en el año 2006 al Foro de Gobernanza de Internet con el siguiente mandato:

"a. debatir temas de políticas públicas relativos a los elementos claves de la gobernanza de *Internet, con objeto de contribuir a la sostenibilidad, la solidez, la seguridad, la estabilidad y el desarrollo de Internet;*

b. facilitar el diálogo entre organismos que se ocupan de políticas públicas internacionales transversales y relacionadas con *Internet, y debatir temas que no se han incluido en el mandato de organismos existentes;*

c. facilitar la comunicación con las organizaciones intergubernamentales apropiadas y otras instituciones en temas de su competencia;

d. facilitar el intercambio de información y de mejores prácticas, y en este sentido aprovechar plenamente las competencias de las comunidades académica, científica y técnica;

e. aconsejar a todas las partes interesadas, sugiriendo soluciones y medios para que *Internet esté disponible más rápidamente y esté al alcance de un mayor número de personas en los países en desarrollo;*

f. Fortalecer y mejorar la participación de las partes interesadas en los mecanismos de gobernanza de *Internet actuales y/o futuros, en particular los de países en desarrollo;*

g. identificar temas emergentes, exponerlos ante los organismos competentes y el público en general, y, en su caso, formular recomendaciones;

h. contribuir a la creación de capacidad para la gobernanza de *Internet en países en desarrollo, aprovechando lo más posible los conocimientos y las competencias locales;*

i. promover y evaluar permanentemente la materialización de los principios de la cmsi en los procesos de gobernanza de *Internet;*

j. debatir temas relativos a los recursos críticos de *Internet, entre otras cosas;*

95 Agenda de Túnez, URL: https://www.itu.int/net/wsis/docs2/tunis/off/6rev1-es.html Consultado el 9 de febrero de 2019.

k. ayudar a encontrar soluciones a los problemas que plantea la utilización correcta o incorrecta de *Internet, que son de particular interés para el usuario común;*

l. publicar sus actas."

Asimismo, se establece en el punto 73 de la Agenda de Túnez que el Foro para la Gobernanza de Internet, debe ser multilateral, democrático, transparente y dejar intervenir a las múltiples partes interesadas. En este sentido, el igf podría (i) beneficiarse y complementarse de las estructuras de la gobernanza de Internet; (ii) constituirse como una estructura sencilla y descentralizada, que se someta a un examen periódico; y (iii) reunirse periódicamente, según se requiera.

Se trabaja a diversos niveles: global, regional y nacional.

El modelo es multistakeholders o de múltiples partes interesadas. Se pone énfasis en que participen todas las partes interesadas. No se toman decisiones, sino que se busca construir mayorías, generar alianzas, transparencia activa y rendir cuentas de forma proactiva.

En lo que respecta a los diversos actores, se suelen identificar tres tipos que trabajan para el adecuado funcionamiento de la red.

Por un lado tenemos aquellos actores que trabajan para el desarrollo de la infraestructura física. Se destaca el rol de la UIT,de la gsma, de la Asociación Iberoamericana de Centros de Investigación y Empresas de Telecomunicaciones (asiet), del Instituto de Ingeniería Eléctrica y Electrónica (ieee), del Grupo de Trabajo de Ingeniería de Internet (ietf por sus siglas en Inglés), así como el rol de las cámaras que agrupan a los operadores de redes y de las autoridades nacionales.

Por otra parte, están aquellos actores vinculados al desarrollo de la infraestructura lógica. A modo de ejemplo:

i. icann, siglas en inglés de "*Internet Corporation for Assigned Names and Numbers"* o "Corporación para la Asignación de Nombres y Números de Internet". Organización sin fines de lucro que opera a nivel internacional y gestiona los dominios de Internet.

ii. iana, siglas en inglés de "*Internet Assigned Numbers Authority*", afiliado de icann, entre sus actividades: administra los nombres de dominio, coordina los

números de ip, proporcionándolos a los registros regionales de Internet, y asigna los números de protocolo de Internet.

iii. W3C, siglas en inglés de "*World Wide Consortium*" o lo que conocemos todos como "www". Es una comunidad internacional que desarrolla estándares web.

iv. iso, siglas en inglés de "*International Organization for Standarization*", es la Organización Internacional de Normalización. Se encarga de promover las normas iso, normas estandarizadas a nivel internacionales, que mejoran la eficiencia y la gestión.

v. Registros de Direcciones de Internet. Hay cinco organizaciones responsables del registro y de la asignación de las direcciones IP: LACNIC para América Latina y el Caribe, APNIC para la región del Pacífico y Asia, ARIN para la región de América del Norte, RIPE NCC para Europa y AFRINIC para África. Asignan y administran los recursos de numeración de Internet (ipv4, ipv6), así como los Números Autónomos y Resolución Inversa para cada una de las regiones, según corresponda.

Finalmente, se encuentran aquellos actores vinculados a aspectos más generales relacionados con el desarrollo social y económico de la población. Se destaca el rol de: (i) los Foros de Gobernanza de Internet de Naciones Unidas, (ii) la Organización para la Cooperación y el Desarrollo Económico (ocde), (iii) la Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura (unesco), (v) Internet Society (isoc), (vi) los gobiernos nacionales, y (vii) representantes de la sociedad civil.

(V.4.) Unión Europea

Se dispone en el artículo 170 del Tratado de Funcionamiento de la Unión Europea (TFUE) que "*1. A fin de contribuir a la realización de los objetivos contemplados en los artículos 26*[96] *y 174*[97] *y de permitir que los ciudadanos de la Unión, los operadores*

[96] Artículo 26 TFUE (antiguo artículo 14 TCE): 1. La Unión adoptará las medidas destinadas a establecer el mercado interior o a garantizar su funcionamiento, de conformidad con las disposiciones pertinentes de los Tratados. 2. El mercado interior implicará un espacio sin fronteras interiores, en el que la libre circulación de mercancías, personas, servicios y capitales estará garantizada de acuerdo con las disposiciones de los Tratados. 3. El Consejo, a propuesta de la Comisión, definirá las orientaciones y condiciones necesarias para asegurar un progreso equilibrado en el conjunto de los sectores considerados."

[97] COHESIÓN ECONÓMICA, SOCIAL Y TERRITORIAL. Artículo 174 (antiguo artículo 158 TCE): "*A fin de promover un desarrollo armonioso del conjunto de la Unión, ésta desarrollará y proseguirá su acción encaminada a reforzar su cohesión económica, social y territorial.*

económicos y los entes regionales y locales participen plenamente de los beneficios resultantes de la creación de un espacio sin fronteras interiores, la Unión contribuirá al establecimiento y al desarrollo de redes transeuropeas en los sectores de las infraestructuras de transportes, de las telecomunicaciones y de la energía.

2. En el contexto de un sistema de mercados abiertos y competitivos, la acción de la Unión tendrá por objetivo favorecer la interconexión e interoperabilidad de las redes nacionales, así como el acceso a dichas redes. Tendrá en cuenta, en particular, la necesidad de establecer enlaces entre las regiones insulares, sin litoral y periféricas y las regiones centrales de la Unión."

Asimismo, en el marco de la Estrategia para el Mercado Unido Digital (MUD) de Europa, comentado en el Capítulo I, se vio como necesario la revisión del marco de las telecomunicaciones, en tanto espina dorsal sobre las cuales se desarrolla el MUD, a fin de reflejar la evolución de la tecnología y del mercado, y adecuar la la normativa (REFIT).

En este sentido, el 11 de diciembre de 2018 se aprobó la Directiva (UE) 2018/1972 del Parlamento Europeo y del Consejo por la que se establece el Código Europeo de las Comunicaciones Electrónicas (CECE).

A través del CECE se busca: (i) incentivar la inversión en redes de banda ancha de alta velocidad, (ii) armonizar la política y la gestión del espectro radioeléctrico, (iii) proteger a los consumidores, (iv) igualar de condiciones para los agentes del mercado, y (v) alcanzar coherencia en la aplicación de las normas[98].

En esta línea, hay tres objetivos primordiales: (1) promover la competencia, (2) impulsar el mercado interior, y (3) atender los intereses de los usuarios finales; para lo cual se tiene que alcanzar: (i) conectividad sostenible a través de redes de muy alta capacidad, (ii) que los servicios se utilicen por todos los ciudadanos y empresas, (iii) precios razonables y asequibles, (iv) competencia leal, (v) innovación, (vi) un uso eficiente del espectro radioeléctrico, (vii) uniformidad y previsibilidad regulatoria, (viii)

La Unión se propondrá, en particular, reducir las diferencias entre los niveles de desarrollo de las diversas regiones y el retraso de las regiones menos favorecidas.
Entre las regiones afectadas se prestará especial atención a las zonas rurales, a las zonas afectadas por una transición industrial y a las regiones que padecen desventajas naturales o demográficas graves y permanentes como, por ejemplo, las regiones más septentrionales con una escasa densidad de población y las regiones insulares, transfronterizas y de montaña."

[98] Considerando (3) del Código Europeo de las Comunicaciones Electrónicas.

normas generales que salvaguarden los intereses de los ciudadanos[99], y (ix) monitoreo y evaluación constante.

Anteriormente el marco regulador para las redes y servicios de comunicaciones electrónicas, estaba formado por cuatro directivas: (i) la Directiva 2002/19/CE del Parlamento Europeo y del Consejo, de 7 de marzo de 2002, relativa al acceso a las redes de comunicaciones electrónicas y recursos asociados, y a su interconexión, (ii) la Directiva 2002/20/CE del Parlamento Europeo y del Consejo, de 7 de marzo de 2002, relativa a la autorización de redes y servicios de comunicaciones electrónicas, (iii) la Directiva 2002/21/CE del Parlamento Europeo y del Consejo, de 7 de marzo de 2002, relativa a un marco regulador común de las redes y los servicios de comunicaciones electrónicas, y (iv) la Directiva 2002/22/CE del Parlamento Europeo y del Consejo, de 7 de marzo de 2002, relativa al servicio universal y los derechos de los usuarios en relación con las redes y los servicios de comunicaciones electrónicas.

Dichas directivas reflejaban el modelo anterior en el que las empresas estaban integradas de forma vertical, participaban tanto en la provisión de redes como de los servicios. Actualmente, la prestación de servicios de comunicaciones ya no está necesariamente unido al desarrollo de una red, el modelo cambió. La convergencia tecnológica hace necesario que se separe la regulación de las redes por un lado, y la regulación de los contenidos por el otro; buscando que todos los servicios y las redes de comunicaciones estén alcanzados por un Código Europeo único, mediante una única Directiva[100].

En este nuevo escenario, el principio de neutralidad tecnológica y reducir la brecha digital es fundamental. No se debe imponer el uso de una determinada tecnología ni favorecer un tipo sobre otro. Cada vez las comunicaciones electrónicas son más fundamentales para el desarrollo de los diversos sectores de la economía, dando forma a nuevas realidades empresariales y sociales, como puede ser el internet de las cosas. Mas para que todo lo anterior sea realmente aplicable, es fundamental conectar a todos, que se desarrollen las habilidades digitales, que se utilice y se confíe en la tecnología.

Se reconoce la necesidad de adaptar las definiciones a fin de responder a la evolución tecnológica y respetar el principio de neutralidad tecnológica. Las redes han

[99] Considerando (23) del Código Europeo de las Comunicaciones Electrónicas.
[100] Considerando (7) del Código Europeo de las Comunicaciones Electrónicas.

evolucionado hacia la tecnología del Protocolo de Internet, dando más posibilidades de elegir a los usuarios y generando una mayor competencia entre los diversos prestadores.

Cada vez más los servicios tradicionales son sustituidos por servicios en línea que ofrecen funciones equivalente, lo cual genera que no se atienda a la tecnología utilizada sino al funcionamiento en sí a efectos de proteger debidamente los diversos derechos en juego. Al usuario le es indiferente si es el proveedor que le brinda el servicio final el mismo que transporta la señal o no[101].

En este sentido, se señala por ejemplo que los servicios de comunicación electrónicas se deben prestar a cambio de una determinada remuneración, pero en la economía digital la información de los usuarios se toma como valor, sustituyendo el pago de dinero por datos personales o de otro tipo de los usuarios. Al respecto se destaca que el Tribunal de Justicia de la Unión Europea (TJUE), en base al artículo 57 del TFUE, ha entendido en Sentencia del 26 de abril de 1988, "Bond van Adverteerders y otros contra Estado Neerlandés", asunto C-352/85, ECLEI:UE:1988:196, que también hay remuneración cuando al proveedor del servicio le paga un tercero; por lo que se entiende que cuando el usuario final es expuesto a anuncios publicitarios como condición para acceder al servicio, el proveedor estaría recibiendo una remuneración.[102]

Asimismo, se señala que para que se considere que hay servicios de comunicaciones interpersonales, los mismos se tienen que dar entre un número finito de personas físicas, donde se realiza intercambio interpersonal, interactivo de información. Alcanza a personas jurídicas en aquellos casos en que las personas físicas actúan en nombre de las personas jurídicas[103].

En definitiva, considerando la realidad actual, al tiempo de simplificar dando más coherencia, accesibilidad e incentivando el despliegue de redes, la innovación y el desarrollo, es que se buscó integrar en un solo texto los actos anteriores, manteniendo ciertas disposiciones inalteradas y ajustando otras, garantizando la libertad de suministrar redes y servicios de comunicaciones electrónicas, estando sujetos a lo dispuesto en el CECE, así como a las limitaciones establecidas en el artículo 52,

[101] Considerando (14) y (15) del Código Europeo de las Comunicaciones Electrónicas.
[102] Considerando (16) del Código Europeo de Comunicaciones Electrónicas.
[103] Considerando (17) del Código Europeo de Comunicaciones Electrónicas.

apartado 1, del Tratado de Funcionamiento de la Unión Europea (TFUE)[104]. Particularmente las vinculadas al orden público, a la seguridad y salud pública; teniendo especialmente en vista que conforme al artículo 52, numeral 1 de la Carta de Derechos Humanos de la Unión Europea (en adelante, "la Carta") prevé que: *"Cualquier limitación del ejercicio de los derechos y libertades reconocidos por la presente Carta deberá ser establecida por la ley y respetar el contenido esencial de dichos derechos y libertades. Dentro del respeto del principio de proporcionalidad, sólo podrán introducirse limitaciones cuando sean necesarias y respondan efectivamente a objetivos de interés general reconocidos por la Unión o a la necesidad de protección de los derechos y libertades de los demás."*

El CECE establece un marco armonizado para la regulación de: (1) las redes de comunicaciones electrónicas, (2) los servicios de comunicaciones electrónicas, y (3) otros recursos y servicios asociados; y dispone el deber de las autoridades nacionales de reglamentación y de otras autoridades competentes, según corresponda, de adoptar determinadas medidas para garantizar la aplicación armonizada del marco regulador en toda la Unión.[105]

Lo que se busca es alcanzar un mercado interior de redes y servicios de comunicaciones electrónicas de muy alta capacidad, que haya una competencia sostenible, interoperabilidad, accesibilidad, seguridad y que todo lo anterior beneficie a los usuarios finales. Asimismo, se quieren garantizar servicios de buena calidad y que sean asequibles, a través de la competencia y de la libertad real de elegir.

Lo anterior se debe complementar con otros actos, como ser: (i) las legislaciones nacionales en relación a este tipo de servicios que sea conforme a la legislación de la Unión, (ii) medidas adoptadas a escala de la Unión para fomentar objetivos de interés general, como por ejemplo: la protección de los datos personales y la privacidad, (iii) actuaciones de los Estados miembros con fines de orden y seguridad pública y de defensa, (iv) los Reglamentos (UE) Nº 531/2012 relativo a la itinerancia en las redes públicas de comunicaciones móviles en la UE[106], (UE) 2015/2120[107] por el cual se

[104] Artículo 52, apartado 1, del TFUE: "Las disposiciones del presente capítulo y las medidas adoptadas en virtud de las mismas no prejuzgarán la aplicabilidad de las disposiciones legales, reglamentarias y administrativas que prevean un régimen especial para los extranjeros y que estén justificadas por razones de orden público, seguridad y salud pública".
[105] Artículo 1 del Código Europeo de Comunicaciones Electrónicas.
[106] Como surge del Artículo 1 de dicho Reglamento, en el mismo se busca garantizar que los usuarios de las redes públicas de comunicaciones móviles que se desplazan dentro de la Unión

introducen medidas en relación con el acceso a una internet abierta y se modifica la Directiva 2002/22/CE referente al servicio universal y a los derechos de los usuarios en relación con las redes y los servicios de comunicaciones electrónicas y el Reglamento (UE) 531/2012 sobre la itinerancia en las redes públicas de comunicaciones móviles en la Unión, y la Directiva 2014/53/UE que trata la armonización de las legislaciones de los Estados miembros sobre la comercialización de equipo radioeléctricos.

Teniendo en cuenta lo expuesto es importante definir los principales conceptos, como son: "red de comunicaciones electrónicas", "servicios de comunicaciones electrónicas", "servicio de acceso a internet", "red de muy alta capacidad".

El artículo 2 de CECE define "redes de comunicaciones electrónicas" como: *"los sistemas de transmisión, se basen o no en una infraestructura permanente o en una capacidad de administración centralizada, y, cuando proceda, los equipos de conmutación o encaminamiento y demás recursos, incluidos los elementos de red que no son activos, que permitan el transporte de señales mediante cables, ondas hertzianas, medios ópticos u otros medios electromagnéticos con inclusión de las redes de satélites, redes fijas (de conmutación de circuitos y de paquetes, incluido internet) y móviles, sistemas de tendido eléctrico, en la medida en que se utilicen para la transmisión de señales, redes utilizadas para la radiodifusión sonora y televisiva y redes de televisión por cable, con independencia del tipo de información transportada"*.

De lo anterior destacamos que son sistemas de transmisión, que permiten el transporte de señales, por diversos medios, como pueden ser: cables, ondas hertzianas, medios ópticos u otros medios electromagnéticos, incluyendo redes satelitales, fijas y móviles. También incluye sistemas de tendido eléctrico, si se utilizan para transmitir

---

no tengan que abonar precios excesivos por los servicios de itinerancia en la Unión, en comparación con precios nacionales competitivos, cuando efectúen y reciban llamadas, cuando envíen y reciban mensajes SMS y cuando utilicen los servicios de comunicaciones de datos por conmutación de paquetes, contribuyendo así al funcionamiento satisfactorio del mercado interior al tiempo que se consigue un elevado nivel de protección de los consumidores, se favorece la competencia y la transparencia en el mercado y se ofrecen tanto incentivos a favor de la innovación como posibilidades de elección a los consumidores.

[107] Tiene por objeto establecer normas comunes destinadas a garantizar un trato eqUITativo y no discriminatorio del tráfico en la prestación de servicios de acceso a internet y a salvaguardar los derechos de los usuarios finales. Su finalidad no es solo proteger a los usuarios finales, sino garantizar simultáneamente el funcionamiento continuado del ecosistema de internet como motor de innovación. En lo que respecta a la itinerancia, se quiere dar confianza a los usuarios para que puedan seguir conectados cuando viajan dentro de la UE, buscando que se conviertan en un motor de convergencia de los precios y de otras condiciones en la UE. (Considerando 1 del Reglamento).

señales, así como otras redes que se utilicen para la radiodifusión, independientemente de la información que se transporte.

Asimismo, el artículo 2 define "servicio de comunicaciones electrónicas" como aquel que es prestado a cambio de una remuneración, a través de redes de comunicaciones electrónicas, y que incluyen a su vez otros tipos de servicios, como son: los servicios de acceso a internet, los servicios de comunicaciones interpersonales y los servicios consistentes, total o principalmente, en el transporte de señales, por ejemplo los utilizados para la prestación de servicios entre máquinas. Se excluyen aquellos servicios que suministran contenidos o que ejerzan control editorial sobre las redes y servicios de comunicaciones electrónicas.

El servicio de acceso a internet es definido en el artículo 2 del Reglamento (UE) 2015/2120, por el que se establecen medidas relacionadas con el acceso a una internet abierta, al servicio universal y a los derechos de los usuarios; como un servicio de comunicaciones electrónicas, que está a disposición del público, a través del cual se proporciona acceso a internet y conectividad, independientemente de la tecnología y de los equipos que se utilicen.

Siguiendo esta línea, vale señalar que los "servicios de comunicaciones interpersonales" son aquellos *"prestados en general a cambio de una remuneración, que permite el intercambio de información directo, interpersonal e interactivo a través de redes de comunicaciones electrónicas entre un número finito de personas, en el que el iniciador de la comunicación o participante en ella determina el receptor o receptores y no incluye servicios que permiten la comunicación interpersonal e interactiva como una mera posibilidad secundaria que va intrínsecamente unida a otro servicio"*[108].

Puede haber servicios interpersonales basados en numeración y otros que sean independientes de la numeración. Los basados en numeración son aquellos que utilizan recursos de numeración pública asignados, del planes de numeración nacional o internacional.

Finalmente interesa destacar que por "servicios asociados" se consideran aquellos "*que permiten o apoyen el suministro, la autoprestación o la prestación de servicios*

[108] Artículo 2.5 del Código Europeo de Comunicaciones Electrónicas.

automatizada a través de dicha red o servicio o tengan potencial para ello e incluyen la traducción de números o sistemas con una funcionalidad equivalente[109]". A modo de ejemplo se señalan los servicios de identidad o de localización.

En lo que respecta a los Objetivos Generales, el CECE busca que los Estados miembros de la UE cumplan con las funciones reguladoras, a través de medidas razonables, necesarias y proporcionadas para que se puedan alcanzar los objetivos, disponiendo que contribuirán para ello: los Estados miembros, la Comisión, el Grupo de política del espectro radioeléctrico (RSPG) y el Organismo de Reguladores Europeos de Comunicaciones Electrónicas (ORECE).

Cada una, dentro de su ámbito de competencia, contribuirá para garantizar la aplicación de políticas destinadas a promover: (i) la libertad de expresión y de información, (ii) la diversidad cultural y lingüística, y (iii) el pluralismo de los medios de comunicación.

Lo que se persigue es[110]:

- Promover la conectividad[111] y el acceso a redes de muy alta calidad[112] por todos los ciudadanos y empresas.

---

[109] Artículo 2.11 del Código Europeo de Comunicaciones Electrónicas.

[110] Artículo 3 del Código Europeo de Comunicaciones Electrónicas.

[111] En el Considerando (23) del Código Europeo de Comunicaciones Electrónicas, se hace referencia a que el marco regulatorio debe perseguir un objetivo adicional de conectividad en forma de resultados: *"acceso generalizado a redes de muy alta capacidad, y utilización generalizada de ella, para todos los ciudadanos y empresas de la Unión, conforma a un precio y una oferta razonables, una competencia eficaz y leal, una innovación abierta, un uso eficiente del espectro radioeléctrico, unas normas comunes y unos planteamientos reguladores previsibles en el mercado interior y las normas sectoriales necesarias para salvaguardar los intereses de los ciudadanos*". Traducen el objetivo de conectividad de la siguiente forma: *"por un lado, en aspirar a unas redes y servicios de la máxima capacidad que sean económicamente sostenibles en una zona determinada y, por otro, en perseguir la cohesión territorial, entendida como la convergencia de la capacidad disponibles en diferentes zonas".* Asimismo, interesa destacar lo señalado en el Considerando (109) del Código Europeo de Comunicaciones Electrónicas, en tanto reconoce que es fundamental la conectividad para el desarrollo económico y social, la participación en la vida pública, la cohesión social y territorial. En esta línea, entienden que la conectividad y las comunicaciones electrónicas se están convirtiendo en elementos integrales de la sociedad y de bienestar, por lo que los Estados deben esforzarse por asegurar que exista cobertura.

[112]Artículo 2 del Código Europeo de Comunicaciones Electrónicas, numeral 2, define "red de muy alta capacidad" como *"una red de comunicaciones electrónicas que se compone totalmente de elementos de fibra óptica, al menos hasta el punto de distribución de la localización donde se presta el servicio o una red de comunicaciones electrónicas capaz de ofrecer un rendimiento de red similar en condiciones usuales de máxima demanda, en términos de ancho de banda disponible para los enlaces ascendente y descendente, resiliencia, parámetros relacionados con*

- Fomentar la competencia en el suministro de redes de comunicaciones electrónicas y recursos asociados, así como en la prestación de los servicios.

- Eliminar las restricciones y facilitar la convergencia para permitir las inversiones en redes y servicios[113].

- Promover los intereses de los ciudadanos, a través de:

    - Conectividad, disponibilidad y adopción de redes de muy alta capacidad y de servicios de comunicaciones electrónicas.

    - Competencia efectiva para maximizar los beneficios, variedad de elección.

    - Seguridad de las redes y servicios.

    - Protección de los usuarios finales, a través de normativa sectorial, a medida, como pueden ser: precios asequibles o las necesidades de determinados grupos sociales –como ser: personas con discapacidad, con más edad y/o con necesidades sociales especiales-.

A efectos de poder cumplir con los objetivos generales establecidos, prevé que las autoridades deben tomar determinadas medidas, así como otras que contribuyan a alcanzar los fines buscados.

Las medidas dispuestas son las siguientes:

- Promover un entorno regulador previsible, estable, revisable y de cooperación[114].

- Garantizar que ante circunstancias similares no haya un trato discriminatorio.

---

los errores, latencia y su variación; el rendimiento de la red puede considerarse similar independientemente de si la experiencia del usuario final varía debido a las características intrínsecamente diferentes del medio a través del cual, en última instancia, la red se conecta al punto de terminación de la red".

[113] Para esto se entiende necesario que se desarrollen normas comunes y enfoques reglamentarios previsibles, así como favorecer: el uso eficaz, eficiente y coordinado del espectro radioeléctrico, la innovación, el establecimiento y desarrollo de redes, el suministro, la disponibilidad e interoperabilidad de redes, el acceso a servicios y la conectividad de extremo a extremo. (Artículo3, apartado 2, literal d)

[114] El ORECE – Organismos Europeos de las Comunicaciones Electrónicas-, el RSPG –Radio Spectum Policy Group- y la Comisión Europea.

- Aplicar el principio de neutralidad tecnológica.
- Fomentar la inversión eficiente orientada al mercado y a la innovación[115].
- Tener en cuenta la variedad de situaciones en cuanto a la infraestructura, a la competencia, a los usuarios finales y, en particular, la realidad de los consumidores en las distintas regiones geográficas.
- Establecer obligaciones ex ante únicamente en cuanto sean necesarias para asegurar la competencia efectiva y sostenible; y ajustándolas o dejándolas sin efecto en cuanto se cumpla la condición.

Finalmente se destaca la importancia de que las autoridades nacionales de reglamentación y aquellas competentes actúen de forma: imparcial, transparente, proporcional y no discriminatoria.

En relación a la coordinación del espectro radioeléctrico, a fin de optimizar el uso y evitar interferencias perjudiciales, se dispone la obligación de los Estados de cooperar entre sí y con la Comisión para realizar la planificación estratégica y la adecuada armonización del uso. Entre los diversos aspectos a considerar, se destacan los económicos, de seguridad, de salud, de interés público, de libertad de expresión, culturales, científicos, sociales y técnicos. Para cumplir con lo anterior, se proponen realizar: (i) mejores prácticas, (ii) facilitar la coordinación, (iii) coordinar la metodología para la asignación y la autorización del uso del espectro.

Los Estados miembros deben velar por el cumplimiento de las misiones establecidas en la Directiva, por una autoridad competente, la cual debe tener como mínimo las siguientes funciones: (a) implementar la reglamentación *ex ante* del mercado, (b) garantizar la resolución de litigios entre empresas, (c) gestionar o tomar decisiones en relación al espectro radioeléctrico, (d) asesorar sobre el mercado y sobre elementos relacionados con la competencia en lo relacionado a los derechos de uso del espectro, (e) proteger al usuario final, (f) supervisar el acceso abierto a internet, (g) evaluar cargas indebidas y el coste del acceso universal, y (h) garantizar que se conserve el número entre proveedores.

[115] Destaca la importancia de tener en cuenta en las obligaciones de acceso, de diversificar el riesgo, permitiendo diferentes modalidades de cooperación entre los inversores y las partes que soliciten el acceso.

Se hace especial énfasis en la importancia de que las autoridades nacionales de regulación, y otras que seas competentes, sean independientes y objetivas, buscando que sean jurídicamente distintas y funcionalmente independientes de cualquier persona física o jurídica proveedora de redes, equipos o servicios de comunicaciones electrónicas. Para el caso de que algún Estado tenga el control o propiedad de una empresa proveedora de redes o servicios de comunicaciones electrónicas, se debe velar por la separación estructural entre la función de prestador y de regulador. Asimismo, se prevé la importancia de que actúen con trasparencia, que no acepten instrucciones de ningún otro órgano, que tengan presupuestos anuales separados y autonomía en su ejecución.

Se quiere promover una mayor coordinación, cooperación y una coherencia reguladora, para lo cual se dispone que las autoridades nacionales deben tener en consideraciones las directrices, dictámenes, recomendaciones, posiciones comunes, así como prácticas y metodologías adoptados por el ORECE.

Interesa destacar que se debe garantizar la libertad de suministrar redes y servicios de comunicaciones electrónicas, y que el acceso a la autorización general para el suministro de redes o servicios de comunicaciones electrónicas, así como para acceder al espectro radioeléctrico y a los recursos de numeración sólo puede estar sometidos a las condiciones que el CECE establece (Anexo I de la Directiva). Las cuales deben ser no discriminatorias, proporcionales y transparentes.

Interesa destacar que tal como dispone el CECE en el Considerando (33), para asegurar la gestión efectiva y la armonización del uso del espectro radioeléctrico, las disposiciones relativas a la gestión espectro radioeléctrico debe ser coherente con lo establecido por las organizaciones internacionales y regionales que se ocupan de la temática, como es la UIT y la Conferencia Europea de Administración Postales y de Telecomunicaciones (CEPT).

A efectos de la transposición de la normativa, se dispone que los Estados miembros deberán adoptar y publicar, a más tardar el 21 de diciembre de 2020, las disposiciones necesarias para el cumplimiento de la directiva, las cuales deberán ser aplicadas a partir de dicha fecha. No obstante, determinadas disposiciones, como ser la coordinación en la asignación de espectro, comenzaron a ser aplicadas a partir del 20 de diciembre de 2018 cuando las condiciones armonizadas hayan sido establecidas por

medidas técnicas de ejecución conforme a la Decisión Nº 676/2002/CE[116], Decisión espectro radioeléctrico, a fin de permitir la utilización del espectro radioeléctrico para las redes y servicios de banda ancha inalámbrica.

Los Estados miembros deben comunicar a la Comisión el texto de las principales disposiciones que adopten en su derecho interno en lo que respecta al ámbito de regulación del CECE.

VI. Consideraciones finales

Las redes de telecomunicaciones, principalmente Internet, junto con el gran desarrollo de las tecnologías, cumplen un rol fundamental en la transformación digital, en tanto son la espina dorsal sobre las cuales se desarrolla todo el ecosistema digital.

Estamos en un momento de constantes cambios, donde el Derecho y la Regulación juegan un rol esencial para dar seguridad, transparencia y previsibilidad. Una mala regulación o que no se ajuste a la realidad, puede afectar mucho a la sociedad, en tanto puede limitar la innovación, el desarrollo, la investigación y desestimular la inversión.

Con el desarrollo de las tecnologías y la convergencia digital, se ha transformado el ecosistema, con múltiples beneficios para los usuarios, en tanto aumenta la competencia, permitiendo que las personas puedan acceder a más servicios, a menores precios.

Los efectos de la convergencia los vemos en las redes, en la forma en que se prestan los servicios, en los dispositivos que utilizamos, así como en la gran variedad de contenidos que podemos compartir y a los que podemos acceder.

Se borran las fronteras y la forma de prestar los servicios evoluciona constantemente, se pueden prestar por diversos medios, siendo esencial que se reconozca el principio de neutralidad tecnológica, así como que se compartan eficientemente los recursos, como ser el espectro radioeléctrico, el espacio físico, el soporte de redes y las redes de acceso y transporte.

[116] Decisión N° 676/2002/CE del Parlamento Europeo y del Consejo, de 7 de marzo de 2002, sobre un marco regulador de la política del espectro radioeléctrico en la Comunidad Europea (Decisión espectro radioeléctrico).

Hay que analizar los supuestos de manera cabal, buscando las respuestas en los principios generales, dejando sin efecto lo que ya no sea necesario, actualizando lo que se requiera y poniendo en el centro a las personas, así como al desarrollo social y económico de todos.

Además, la naturaleza global de Internet y la rapidez con la que se producen los cambios, hacen que la coordinación internacional, el modelo *multistakeholders* y la autorregulación, cobren cada vez mayor relevancia.

Asimismo, se muestra cada vez más la necesidad de simplificar y armonizar, dar previsibilidad y seguridad, a fin de promover la innovación y el desarrollo.

Toma mayor relevancia:; (i) la necesidad de que los reguladores sean independientes, que actúen de forma imparcial, objetiva, transparente, no discriminatoria y proporcionada; (ii) la compartición de infraestructura y la gestión adecuada de los recursos, como ser la armonización y la coordinación en el uso del espectro radioeléctrico y de la numeración; y (iii) la coordinación, el diálogo y el intercambio tanto a nivel nacional, como regional e internacional.

En definitiva, se presentan cambios económicos y sociales de gran magnitud, que implican grandes beneficios para las personas, al tiempo que generan riesgos para los derechos fundamentales y para la economía tradicional si no se toman medidas adecuadas y se ajustan las regulaciones. Se debe buscar que los derechos fundamentales se respetan tanto *online* como *offline,* que no se generen ventajas competitivas a consecuencia de asimetrías regulatorias, y que los mismos servicios, independientemente del medio a través del cual se brinden, tengan las mismas regulaciones.

La forma no es prohibir o establecer regulaciones sin sentido, tenemos que repensar los modelos. Hay que darle la bienvenida a la innovación y promoverla, siendo fundamental el trabajo en conjunto entre especialistas de diferentes disciplinas, así como la debida coordinación entre los diversos actores del sector, a nivel internacional, regional y nacional. Debemos apoyarnos en los principios generales, en los modelos *multistakeholders* y en la autorregulación.

CAPÍTULO III: BASES JURÍDICAS Y DISEÑO INSTITUCIONAL DE LOS SERVICIOS DE TELECOMUNICACIONES EN EL URUGUAY Y EN ESPAÑA

I. Introducción

Como hemos enfatizado anteriormente, estamos ante una nueva realidad, la digital, la cual impacta a todos, en todo y lo hace a una velocidad exponencial.

Las redes de telecomunicaciones se presentan como base para la transformación digital. En tanto la nueva realidad se desarrolla sobre Internet, se requiere que se desplieguen redes de última generación, con capacidad y calidad suficiente; siendo esencial que se realicen inversiones, que se impulse el desarrollo y la innovación, al tiempo que se generen marcos jurídicos que otorguen reglas claras, previsibilidad, seguridad, y que reflejen la realidad y las necesidades.

Se suelen plantear diversas dificultades a la hora de desplegar las redes de telecomunicaciones, por lo que la tendencia apunta a que se compartan los recursos, facilitando el acceso universal, el despliegue de redes, el uso eficiente del espectro, así como que se respete y promueva la neutralidad tecnológica, buscando ajustar los marcos jurídicos para responder adecuadamente a la nueva realidad, a fin de dar seguridad, transparencia y promover la inversión.

Hay diversas formas de regular, mas considerando la velocidad con la que se producen los cambios tecnológicos, así como que debemos estimular la innovación, el desarrollo y el despliegue; el trabajo en conjunto entre los diversos actores –públicos, privados, sociedad civil, reguladores, academia, etc., tanto a nivel internacional, regional, como nacional– se presenta cada vez más como la mejor alternativa, en tanto facilita la participación de todos, la coordinación y la compartición de recursos, lo cual permite alcanzar mejores resultados en menores tiempos.

Tal como se desarrolló en el Capítulo I, surge de las diversas Agendas Digitales, la necesidad de brindar conectividad de calidad a todas las personas. El despliegue de redes, fortalecer la infraestructura, universalizar el acceso, alcanzar mejoras en la capacidad y calidad, atender el dinamismo tecnológico y el desarrollo de nuevos servicios digitales, se presentan como bases fundamentales para el adecuado desarrollo del mundo digital.

Sin perjuicio, para que lo anterior sea posible, se requiere el trabajo conjunto y la coordinación de diversos actores de la sociedad, así como que se realicen múltiples inversiones. En este sentido, es fundamental que el marco regulatorio otorgue seguridad, transparencia, previsibilidad, reglas de juego claras; al tiempo que responda a la realidad y a las necesidades de la tecnología, del mercado, en vistas de alcanzar el interés general.

Considerando lo expuesto, se desarrollará en el presente capítulo las bases de la regulación en Uruguay y en España en lo que respecta a los servicios de telecomunicaciones, así como lo vinculado al diseño institucional, a las licencias para prestar los servicios, así como los derechos y obligaciones de quienes brindan los mismos.

Como se verá, son regímenes jurídicos muy distintos, el de España se ha liberalizado y simplificado como forma de universalizar los servicios y de promover la libre competencia. El régimen uruguayo, si bien los principios son bastante similares a los establecidos en España, las autorizaciones o licencias son por clase de servicio, estableciendo la tecnología a través de la cual se deben brindar los mismos. Asimismo, no se prevé la compartición de infraestructuras ni de recursos, y si bien se supone que hay libre competencia, en los hechos hay un operador público que detenta el monopolio en algunos servicios y no hay contabilidad separada. A todas luces el régimen uruguayo requiere de una actualización a fin de reflejar la realidad y las necesidades actuales.

II. Bases de la regulación de telecomunicaciones en Uruguay[117]

La prestación de los servicios, así como la instalación, el uso y la explotación de los mismos en dicho país se rige por lo establecido en la Constitución de la República Oriental del Uruguay (la Constitución), los convenios y tratados internacionales de los que Uruguay sea parte, el ordenamiento jurídico vigente –comprendiendo los principios generales de derecho, las leyes, decretos, reglamentos y resoluciones–, así como por las normas complementarias que se dicten por la Unidad Reguladora de Servicios de Comunicaciones (URSEC). Siendo fundamental tener presente que la enumeración de derechos, deberes y garantías realizada, no excluye los que son inherentes a la

117 Véase nuestro trabajo en ARAMENDÍA, MERCEDES, "Aspectos fundamentales de los servicios de telecomunicaciones en el país" en *Estudios de Telecomunicaciones y Sociedad de la Información,* Universidad de Montevideo, 2018, pp. 55 y ss.

personalidad humana o que se derivan de la forma republicana de gobierno (Artículo 72 de la Constitución); y que los preceptos que reconocen derechos a los individuos y que atribuyen facultades y deberes a las autoridades, no dejarán de aplicarse por falta de reglamentación, sino que serán suplidos recurriendo a los fundamentos de leyes análogas, a los principios generales de derecho y a la doctrina generalmente admitida (Artículo 332 de la Constitución).

Los tres postulados fundamentales del Derecho de la Regulación Económica son: (1) la propiedad y la posesión privada, (2) la libertad de elección por los particulares, empresas y corporaciones en la colocación y uso de sus recursos, (3) el mercado como escenario de los negocios y las decisiones económicas.

Como señalan los doctores Brito y Delpiazzo "…*al Derecho de la Regulación Económica corresponde operar definiendo normativamente los requisitos conceptuales para la libertad económica. Pero también, los reclamos de la dimensión de moralidad – con la búsqueda de la igualdad efectiva reclamada desde la dignidad común a todos los hombres– se hacen presentes con una fundamental carga de sentido a la hora de la regulación económica y el control estatal*"[118].

Como enseñan los nombrados catedráticos[119], el Derecho de la Regulación Económica actúa entre la libertad y la autoridad, buscando el desarrollo, el crecimiento económico y la reducción de la pobreza; habiendo más probabilidades de alcanzar lo anterior cuando el gobierno actúa como complemento del mercado, y ocurriendo fracasos cuando se enfrentan.[120]

No es cuestión de ir al intervencionismo estatal o al liberalismo económico, sino que lo que ha demostrado tener más eficiencia para producir y distribuir, es la libre competencia, en tanto otorga los incentivos para la innovación y la evolución de la tecnología. Sin embargo, los marcos jurídicos, que solo el Estado puede establecer, son importantes para el funcionamiento de los mercados. En definitiva, como enseñan los

118 BRITO, MARIANO Y DELPIAZZO, CARLOS, "Bases Fenoménicas" en *Derecho Administrativo de la Regulación Económica,* Universidad de Montevideo, 1998, pp. 18.

119 BRITO, MARIANO Y DELPIAZZO, CARLOS, "Bases constitucionales" en *Derecho Administrativo de la Regulación Económica,* Universidad de Montevideo, 1998, pp. 21.

120 CONABLE, BARBER B., Presidente del Banco Mundial: Prefacio del "Informe sobre el desarrollo mundial 1991 - La tarea acuciante del desarrollo", (Washington, EE.UU., 1991) citado por BRITO, MARIANO R. Y DELPIAZZO, CARLOS, obra citada, pp. 21.

nombrados: *"No se trata de elegir entre el Estado y el mercado, sino que cada una de ellos tiene una función importante e irremplazable que cumplir"*[121].

Partiendo de las premisas expuestas, en el mercado de telecomunicaciones deberían confluir los tres pilares fundamentales del Derecho Administrativo Económico. Por un lado la propiedad y la posesión privada, por otro, la libertad de elección que tienen las personas y empresas en la colocación y uso de sus recursos, y finalmente, el mercado como escenario de los negocios y de las decisiones económicas. Todo lo anterior en un marco jurídico que, partiendo de la Constitución, de los principios generales de derecho y de las demás disposiciones de derecho, otorgue seguridad, previsibilidad y reglas de juego claras, lo cual es fundamental para desarrollar la confianza, generando más inversiones y oportunidades para todos.

En el caso de las telecomunicaciones, nos encontramos en la esfera de la "actuación estatal en el ámbito de la actividad privada"[122], nos referimos a actividades en el ámbito comercial e industrial, en las que la Administración Pública desempeña las actividades, ya sea: (i) mediante autorización expresa o mediante la nacionalización de empresas o participando en la entidad privada; (ii) desplazando a los particulares, en caso de monopolio, o actuando en concurrencia, en libre competencia; (iii) régimen de derecho privado, dentro del ámbito del derecho público por el interés que tiene la actividad en la población y para alcanzar el interés general.

Cuando la Administración presta servicios industriales y comerciales, requiere ley que le autorice a poder prestar estos servicios por los principios de especialidad y de legalidad, contrario a lo que ocurre con los particulares que se rigen por el principio de libertad, pudiendo hacer todo aquello que no esté prohibido por ley por razones de interés general (artículos 7, 10 y 36 de la Constitución), el Estado por el contrario requiere de una ley que expresamente le autorice a poder brindar ese servicio (artículo 190 de la Constitución).

El principio que rige estas actividades es el de libre concurrencia, comprendido en la libertad de industria y comercio, así como el derecho de todas las personas de dedicarse a las distintas actividades comerciales e industriales (arts. 7, 10 y 36 de la

121 CONABLE, BARBER B., citado por los doctores BRITO, MARIANO R. Y DELPIAZZO, CARLOS, obra citada, pp. 21.

122 DELPIAZZO, CARLOS, *Derecho Administrativo Especial,* vol. 2, segunda edición, Amalio M. Fernández. Montevideo, 2009, pp. 197 y ss.

Constitución). Las empresas operan en un régimen de economía de mercado basado en la libertad de actuación, siendo el mercado el ámbito donde se accede a los distintos bienes y servicios, donde las empresas compiten, ofreciendo a los ciudadanos más opciones a menor precio, actuando el Estado para corregir aquellas actuaciones que perjudican a la competencia o a los consumidores.

La regla es la libertad y la libre competencia, los límites: (i) son la excepción, (ii) requieren ley, que sea aprobada por razones de interés general y, en el caso de que establezcan monopolios, deben estar aprobados además por mayorías especiales –artículo 85, numeral 17 de la Constitución–, y (iii) deben ser interpretados de forma restrictiva.

Previo a profundizar en el marco jurídico, vale señalar que el ordenamiento jurídico de Uruguay adopta la definición de "telecomunicaciones" dispuesta en el Convenio Internacional de Telecomunicaciones de 1973, y las define como *"toda transmisión, emisión o recepción de signos, señales, escritos o imágenes, sonidos o informaciones de cualquier naturaleza por hilo, radioelectricidad, medios ópticos u otros sistemas electromagnéticos*"[123].

(II.I) Objeto y fin de la prestación de los servicios de telecomunicaciones[124]

El ordenamiento jurídico de Uruguay establece los objetivos y los principios en base a los cuales se debe desarrollar la actividad de telecomunicaciones en dicho país.[125]

Los mismos están establecidos específicamente en el artículo 72 de la Ley Nº 17.296, en la redacción dada por la ley 19.889, y en el artículo 4 del Reglamento de Licencias de Telecomunicaciones, aprobado por el Decreto Nº 115/003. Asimismo, debemos tener siempre presente lo establecido los artículos 7, 10, 36, 72 y 332 de la Constitución, así como en el Decreto Nº 500/91.

Vale destacar que en virtud de lo establecido en el Artículo 345 de la ley Nº 13.318 y el Artículo 23 literal a) del Decreto-Ley Nº 15.524, los principios generales

123 DELPIAZZO CARLOS, *Lecciones de Derecho Telemático,* Tomo I, Fundación de Cultura Universitaria, Montevideo, 2009, pp. 9.

124 Véase nuestro trabajo en ARAMENDÍA, MERCEDES, "Aspectos fundamentales de los servicios de telecomunicaciones en el país" en *Estudios de Telecomunicaciones y Sociedad de la Información,* Universidad de Montevideo. Montevideo, 2018, pp. 55 y ss.

125 DELPIAZZO, CARLOS, *Derecho de las telecomunicaciones*, Universidad de Montevideo, Año 2005, pp. 40.

constituyen regla de Derecho[126], y sirven como criterio de interpretación para colmar lagunas y vacíos normativos.[127]

En este sentido, las actividades de telecomunicaciones se deben cumplir de conformidad con los siguientes objetivos:

- La extensión y universalización del acceso a los servicios.
- El fomento del nivel óptimo de la inversión para la prestación de los servicios en las condiciones que fije la regulación sectorial.
- La protección de los derechos de los usuarios y consumidores.
- La promoción de la libre competencia en la prestación, sin perjuicio de los monopolios y exclusividades legalmente dispuestos.
- La prestación no discriminatoria, con regularidad, continuidad y calidad de los servicios.
- La libre elección por los usuarios entre los diversos prestadores, en base a información clara y veraz.
- La aplicación de tarifas que tomen en consideración la evolución de los costos y otros criterios técnicos correspondientes, sin perjuicio de los lineamientos respecto a la política tarifaria que el Poder Ejecutivo incorpore.

Asimismo, el Artículo 4 del Reglamento de Licencias, aprobado por el Decreto N° 115/003, establece los siguientes "*Principios y Derechos Generales*" para la actividad y prestación de los servicios:

- Libre elección: derecho que tienen los usuarios a elegir. Los prestadores no pueden limitar, impedir o distorsionar este derecho. A estos efectos, se debe atender también lo establecido en la Ley Nº 17.250: Relaciones de Consumo y Defensa del Consumidor.

126 CAJARVILLE PELUFFO, JUAN PABLO, "Reflexiones sobre los principios generales de Derecho en la Constitución uruguaya" en *Estudios Jurídicos en memoria de Alberto Ramón Real* (F.C.U., Montevideo, 1996), pp. 173 y ss, citado por DELPIAZZO, CARLOS en obra citada, pp. 40.

127 FRUGONE SCHIAVONE, HÉCTOR, "Principios del procedimiento Administrativo", en *El nuevo procedimiento administrativo*, pp. 31, citado por DELPIAZZO, CARLOS en obra citada, pp. 40.

- Neutralidad Tecnológica: libertad para adoptar tecnologías para la prestación de los servicios. Este principio es esencial para el adecuado desarrollo de los servicios de telecomunicaciones, implica que no se regulan tecnologías, lo cual parece lógico en tanto ex ante es muy difícil poder prever el desarrollo que vendrá. El intentar atar servicios a una determinada tecnología, solo puede implicar límites a la innovación y al desarrollo, dado que se limita la evolución de las formas en que ese mismo servicio puede ser brindado.

- Libre y sana competencia: los prestadores de servicios no pueden llevar a cabo prácticas que puedan restringir, impedir u obstaculizar la competencia, ni establecer condiciones que generen situaciones desventajosas o discriminatorias entre los distintos licenciatarios. Se debe atender lo establecido en la Ley Nº 18.159, Defensa de la Libre Competencia, y su Decreto Nº 404/007.

- Continuidad: la prestación del servicio debe ser sin interrupciones, excepto las debidamente justificadas.

- Generalidad: prestar el servicio en el área autorizada, a quien lo requiera y esté en condiciones de acceder a él.

- Igualdad: no incurrir en prácticas discriminatorias, debiéndose realizar la categorización por razones objetivas.

- Regularidad: la prestación debe ser en buenas condiciones técnicas y con calidad satisfactoria.

(II.II) Diseño institucional de los servicios de telecomunicaciones[128]

La importancia que tienen los servicios de telecomunicaciones para alcanzar el interés general, así como la diversa participación del Estado en la actividad, hace esencial que se respete en su plenitud el sistema de frenos y contrapesos, la división de poderes y el Estado de Derecho.

En esta línea, más allá de lo establecido en la Constitución, se han dictado diversas leyes que han creado organismos y direcciones sectoriales con competencias

128 Véase nuestra obra en ARAMENDÍA, MERCEDES, "Sujetos y organismos nacionales con competencia en los servicios de telecomunicaciones y en los servicios de comunicación audiovisual" en *Estudios de Telecomunicaciones y Sociedad de la Información*, obra colectiva, coordinada junto con la Dra. Vázquez, Cristina. Universidad de Montevideo. Montevideo, 2018, pp. 125 y ss.

específicas en la materia. En este marco y en vista del principio de especialidad, el Estado define políticas en línea con la Constitución y las leyes, y participa en el mercado, siendo esencial la igualdad entre los diversos actores, por medio de la regulación y del control, así como la coordinación a fin de fomentar el desarrollo y alcanzar el bien común.

(II.II.1) Poder Ejecutivo - Ministerio de Industria, Energía y Minería (miem)

Conforme a lo establecido en el artículo 168, numeral 4, de la Constitución le compete ejecutar y hacer ejecutar las leyes, expidiendo los reglamentos que sean necesarios[129].

En esta línea, el artículo 94 de la Ley 17.296 dispone que es "*competencia exclusiva del Poder Ejecutivo a través del Ministerio de Industria, Energía y Minería, la fijación de la política nacional de telecomunicaciones y servicios de comunicación audiovisual"* y el artículo 1° del Decreto N° 155/2005 señala que *"Las competencias del Poder Ejecutivo en materia de Comunicaciones y Telecomunicaciones serán ejercidas con la intervención del miem."*

En línea con lo anterior, dentro del Poder Ejecutivo, el miem es a quien le compete la materia de telecomunicaciones.

Al respecto, el miem debe hacer cumplir la Constitución, las leyes, decretos y resoluciones en los temas de su cartera[130].

El artículo 94 de la Ley N° 17.296, en la redacción dada por el artículo 147 de la Ley N° 18.719 y por el artículo 142 de la Ley N° 18.996, dispone que en relación a las telecomunicaciones le compete al Poder Ejecutivo los siguientes cometido:

a. Aprobar convenios con entidades extranjeras.

b. Autorizar el funcionamiento de estaciones de radiodifusión de amplitud modulada (am), frecuencia modulada (fm), televisión abierta y televisión para abonados.

c. Autorizar genéricamente la asignación de frecuencias por parte de la URSEC, para servicios diferentes a los del literal B), por la modalidad de subasta u otro procedimiento competitivo.

129 Numeral 4, Artículo 168 de la Constitución de la República Oriental del Uruguay.
130 Artículo 181 de la Constitución.

d. Habilitar genéricamente la prestación de determinados servicios de telecomunicaciones por particulares.

e. Fijar los precios que deberán abonar los concesionarios por la utilización o aprovechamiento de frecuencias radioeléctricas y demás bienes escasos necesarios.

f.Imponer sanciones, como ser: (i) decomiso de los elementos utilizados para cometer la infracción o de los bienes detectados en infracción, cuando sea accesoria, (ii) multa, (iii) suspensión de hasta noventa días en la prestación de la actividad, y (iv) revocación de la autorización o concesión.

(II.II.2) Dirección Nacional de Telecomunicaciones y Servicios de Comunicación Audiovisual (DINATEL)

La dinatel fue creada por el artículo 172 de la Ley N° 17.930, redacción dada por el artículo 333 de la Ley N° 19.355. Sus cometidos y objetivos están establecidos en el Decreto N° 519/009, en el artículo 94 Bis de la Ley N° 17.296, redacción dada por el artículo 418 de la Ley N° 18.719, y en el artículo 64 de la Ley Nº 19.307.

Tiene como objetivos estratégicos formular, articular y coordinar las políticas de telecomunicaciones y de servicios de comunicación audiovisual, así como asesorar y representar al Poder Ejecutivo y a todo otro organismo estatal que lo requiera en la materia.

Entre sus competencias se encuentran las siguientes[131]:

a. Realizar propuestas y asesorar en la fijación de la política nacional.

b. Instrumentar, coordinar y monitorear el cumplimiento.

c. Diseñar políticas y planificar la gestión del espectro radioeléctrico.

d. Asesorar en las políticas y criterios para otorgar licencias y autorizaciones.

e. Dictaminar preceptivamente en procedimientos de concesión y autorización.

f.Asesorar sobre la administración de los recursos para el despliegue de tecnologías de información y comunicación.

131 Artículo 94-BIS de la Ley N° 17.296, agregado por el artículo 418 de la Ley N° 18.719.

g. Propiciar estudios, análisis y realizar el monitoreo de la situación del sector.

h. Recabar directamente la información necesaria para cumplir sus cometidos.

i. Desarrollar mecanismos de consulta para conocer opiniones.

j. Promover acciones para mejorar el despliegue tecnológico.

k. Asesorar al Poder Ejecutivo en materia de acuerdos internacionales.

l. Representar al Poder Ejecutivo en grupos de trabajo.

m. Coordinar el cumplimiento de las políticas públicas y los objetivos estratégicos.

(II.II.3) Unidad reguladora de servicios de comunicaciones (URSEC)

El 9 de julio de 2020 se promulgó la Ley N° 19.889, conocida como la Ley de Urgente Consideración (en adelante, "LUC"), por medio de la cual, entre otros cambios, se modificó la naturaleza jurídica de la URSEC a fin de transformarla en un regulador más fuerte e independiente.

El artículo 256 de la LUC sustituye el artículo 70 de la ley 17.296 de 21 de febrero de 2001 -el cual había creado a la URSEC como un órgano desconcentrado del Poder Ejecutivo, sin perjuicio de su facultad de avocación- y crea a la URSEC como un persona jurídica estatal descentralizada, como un servicio descentralizado.

Hasta la entrada en vigencia de la LUC, la URSEC estaba dentro del sistema orgánico Poder Ejecutivo, con la modificación pasa a ser una persona jurídica estatal menor, dentro de un marco que acentúa el reparto de competencias, diferenciando: (a) la planificación y fijación de políticas a cargo del Poder Ejecutivo[132], (b) la regulación y el control a cargo de un organismo independiente y especializado, y (c) la prestación de la actividad concreta, tanto por operadores públicos como privados.[133]

[132] CAJARVILLE, JUAN PABLO, "El Poder Ejecutivo como conductor de políticas sectoriales en la legislación uruguaya" en *Estudios de Derecho Administrativo en homenaje al Centenario de la Cátedra de Derecho Administrativo*, tomo II, Montevideo, 1979, pp. 72 y ss. Citado por BRITO, MARIANO y DELPIAZZO, CARLOS, obra citada, pp. 63.

[133] DELPIAZZO, CARLOS, "Desafíos actuales del control", Fundación de Cultura Universitaria, Montevideo, 2001, pp. 15.

Tiene competencias específicas relacionadas con los servicios de telecomunicaciones, con el correo postal y con los servicios de comunicación audiovisual.

Sus competencias las debe cumplir de conformidad con los objetivos y las políticas definidos por el Poder Ejecutivo, quien reglamenta los procedimientos a tales efectos.

El artículo 262 de la LUC sustituye el artículo 75 de la Ley N° 17.296 y dispone que la URSEC estará dirigida por un Directorio integrado por tres miembros designados de conformidad con el artículo 187 de la Constitución de Uruguay, quiénes durarán seis años en sus cargos y la representación la tendrá el Presidente del Directorio.

Anteriormente los miembros eran designados por el Presidente de la República actuando en Consejo de Ministros entre personas que por sus antecedentes personales, profesionales y conocimiento en la materia, aseguren independencia de criterio, eficiencia, objetividad e imparcialidad en su desempeño. Tras la modificación, los miembros deben ser designados por el Presidente de la República en acuerdo con el Consejo de Ministros, previa venia de la Cámara de Senadores, otorgada sobre propuesta motivada en las condiciones personales, funcionales y técnicas, por un número equivalente a tres quintos de los componentes de dicha cámara conforme a lo establecido en el inciso primero del artículo 94 de la Constitución.

El plazo del mandato de los miembros del directorio continúa siendo de seis años, lo cual permite que la finalización del plazo no coincida con los actos electorales.

Respecto a las cualidades de las personas propuestas, considero que son similares y en ambos casos debe motivarse. Si bien se utilizan términos diferentes, reflexiono que son sinónimos y que la independencia de criterio, eficiencia, objetividad e imparcialidad son principios que rigen la actuación del Regulador y que se desprenden del Decreto 206/2002 que aprobó el Código de Ética del Regulador.

Al respecto, los principios generales que rigen su actuación son los siguientes: (i) probidad, (ii) templanza, (iii) equidad, (iv) legalidad, (v) diligencia, (vi) idoneidad, (vii) transparencia, (viii) veracidad, (ix) responsabilidad.

Complementando, los principios particulares son los siguientes: (i) imparcialidad, (ii) capacitación, (iii) ponderación, (iv) reserva, (v) autonomía técnica e independencia de criterio, (vi) uso adecuado de los bienes del Estado, (vii) uso adecuado del tiempo de

trabajo, (viii) colaboración, (ix) obligación de denunciar, (x) dignidad y decoro, (xi) obligación de honrar el buen nombre y prestigio de la institución, (xii) tolerancia, (xiii) buena fe y lealtad.

En la LUC no se hace referencia expresa a la posibilidad de que los directores sean reelectos, como sí se hacía en la redacción anterior, sin perjuicio debe considerarse lo establecido en el último inciso del artículo 192 de la Constitución que establece la posibilidad de que los miembros de los Directorios puedan ser reelectos o designados para otro Directorio siempre que su gestión no haya merecido observación del Tribunal de Cuentas, emitido por lo menos por cuatro votos conformes de su miembro.

Vale comentar que el artículo 645 del Proyecto de Ley de Presupuesto remitido por el Poder Ejecutivo el 31 de agosto de 2020 establece las atribuciones del Directorio de la URSEC, sin perjuicio de otras facultades jurídicas necesarias para el adecuado ejercicio de la competencia del organismo. Expresamente señala las siguientes facultades:

Ejercer la dirección superior administrativa, técnica e inspectiva, y el control de todos los servicios a su cargo.

Aprobar las reglamentaciones necesarias para la organización y funcionamiento del organismo, así como estructura organizativa.

Designar, promover, trasladar, cesar o destituir a los funcionarios de su dependencia, pudiendo realizar las contrataciones que fueran necesarias, y ejercer la potestad disciplinaria sobre todo el personal, todo ello de acuerdo a la normativa vigente.

Adquirir, gravar, enajenar y realizar todo otro acto jurídico necesario sobre toda clase de bienes muebles e inmuebles.

Asimismo señala que el Presidente del Directorio puede adoptar las medidas urgentes cuando fueren imprescindibles e impostergables, dando cuenta al Directorio en la primera sesión, a realizarse dentro de los primeros diez días hábiles siguientes al de la adopción de la medida, y estándose a lo que éste resuelva.

En caso de ausencia o incapacidad del Presidente o si quedara vacante el cargo, las funciones serán ejercidas transitoriamente por el Vicepresidente.

Cabe destacar la referencia a que los miembros del Directorio deben velar por el respeto a la Constitución, las leyes y los reglamentos en el dictado de sus resoluciones.

Finalmente, vale destacar que conforme el artículo 24 de la Constitución, como persona jurídica, servicio descentralizado, la URSEC es civilmente responsable por el daño causado a terceros, en la ejecución de los servicios públicos, confiados a su gestión o dirección. En esta línea, interesa subrayar que conforme al artículo 25 de la Constitución, cuando el daño haya sido causado por sus funcionarios, en el ejercicio de sus funciones o en ocasión de ese ejercicio, en caso de haber obrado con culpa grave o dolo, el organismo podrá repetir contra ellos lo que hubiere pagado en reparación.

Conforme a lo establecido en el artículo 190 de la Constitución, la URSEC solo puede desempeñar las competencias que por ley se le hayan asignado.

En relación a las actividades de telecomunicaciones y postales tiene una competencia muy extensa y detallada en la LUC, la cual comprende principalmente aspectos regulatorios, de control y punitivos a fin de asegurar el cumplimiento de las disposiciones sectoriales, a la luz de los objetivos de la URSEC.

Sin perjuicio de lo dispuesto en la LUC, la URSEC también tiene otras competencias que le han sido asignadas por otras leyes nacionales, como ser por la Ley N° 19.307 de Servicios de Comunicación Audiovisual o por el artículo 14 de la Ley N° 18.910, modificada por el Artículo 6 de la Ley N° 19.593, en relación a la compatibilidad e interoperabilidad de las redes de terminales de procesamiento electrónico de pagos y la interconexión de dichas redes con los emisores de medios de pago electrónicos y adquirentes, así como el correcto y seguro funcionamiento de dicho sistema de pagos electrónicos.

Es importante tener presente que el artículo 332 de la Constitución dispone que *"Los preceptos de la presente Constitución que reconocen derechos a los individuos, así como los que atribuyen facultades e imponen deberes a las autoridades públicas, no dejarán de aplicarse por falta de reglamentación respectiva, sino que ésta será suplida, recurriendo a los fundamentos de leyes análogas, a los principios generales de derecho y a las doctrinas generalmente admitidas".*

Respecto a los servicios de telecomunicaciones, el artículo 259 de la LUC sustituye el artículo 73 de la Ley N° 17.296, en la redacción dada por el artículo 142 de

la Ley N° 18.719, y dispone que la URSEC, de conformidad con las políticas definidas por el Poder Ejecutivo, tiene las siguientes competencias:

A) La regulación y control de las actividades en materia de telecomunicaciones, así como de los respectivos operadores.

B) Velar por el cumplimiento de las normas sectoriales específicas.

C) Administrar, defender y controlar el espectro radioeléctrico nacional.

D) Otorgar:

1) Autorizaciones precarias para el uso de frecuencias del espectro radioeléctrico nacional, así como para la instalación y operación de estaciones radioeléctricas excepto las previstas en el literal B) del artículo 94 de la ley 17.296.

2) Sin perjuicio de lo anterior, cuando previa autorización del Poder Ejecutivo, y conforme al reglamento a dictar por el mismo, se asigne el uso de frecuencias por la modalidad de subasta u otro procedimiento competitivo, deberá comunicarse en el llamado a interesados, el plazo de vigencia de la autorización que a tal efecto indique el Poder Ejecutivo y sus garantías de funcionamiento, bases sobre las cuales se autorizará el uso de las frecuencias.

3) Los servicios autorizados en el numeral 1) estarán sometidos al control del autorizante, en todos los aspectos de su instalación y funcionamiento.

E) Controlar la instalación y funcionamiento, así como la calidad, regularidad y alcance, de todos los servicios de telecomunicaciones, sean prestados por operadores públicos o privados.

F) Formular normas para el control técnico y manejo adecuado de las telecomunicaciones, así como controlar su implementación.

G) Fijar reglas y patrones industriales que aseguren la compatibilidad, interconexión e interoperabilidad de las redes, incluida la red pública, así como el correcto y seguro funcionamiento de los equipos que se conecten a ellas, controlando su aplicación.

H) Presentar al Poder Ejecutivo para su aprobación, proyectos de reglamento y de pliegos de bases y condiciones para la selección de las entidades autorizadas al uso de

frecuencias radioeléctricas, conforme con lo establecido en el numeral 3) del literal D) del presente artículo.

I) Ejercer la supervisión técnica y operativa de las emisiones de radiodifusión y de televisión, cualesquiera fuere su modalidad.

J) Mantener relaciones internacionales con los organismos vinculados a su ámbito de competencia.

K) Hacer cumplir la presente ley, sus reglamentaciones, disposiciones emanadas de ella misma y actos jurídicos habilitantes de la prestación de servicios comprendidos dentro de su competencia.

L) Asesorar al Poder Ejecutivo respecto a los requisitos que deberán cumplir quienes realicen actividades comprendidas dentro de su competencia.

M) Dictaminar preceptivamente en los procedimientos de concesión y autorización para prestar servicios comprendidos dentro de su competencia, los que deberán basarse en los principios generales de publicidad, igualdad y concurrencia.

N) Ejercer la potestad normativa mediante el dictado de actos administrativos para el ejercicio de su competencia en materia de regulación y control de las actividades y servicios que le correspondan.

O) Requerir a los prestatarios públicos y privados, todo tipo de información para el cumplimiento de sus cometidos.

P) Dictar normas técnicas con relación a dichos servicios.

Q) Controlar el cumplimiento por parte de los operadores públicos y privados, prestadores de servicios comprendidos dentro de su competencia, de las normas jurídicas y técnicas aplicables, pudiendo requerirles todo tipo de información.

R) Recibir, instruir y resolver las denuncias y reclamos en materia de defensa de la competencia, de conformidad con lo dispuesto en el artículo 27 de la Ley N° 18.159, de 20 de julio de 2007.

S) Proteger los derechos de usuarios y consumidores, pudiendo ejercer las atribuciones conferidas a las autoridades administrativas por la Ley N° 17.250, de 11 de agosto de 2000.

T) Determinar técnicamente las tarifas y precios sujetos a regulación de los servicios comprendidos dentro de su competencia, elevándolos al Poder Ejecutivo para su consideración y aprobación. La tarifa de interconexión deberá establecerse de común acuerdo entre las partes, y si no existe acuerdo lo resolverá la Unidad Reguladora.

U) Aplicar las sanciones previstas en los literales a), b), c), d), e) y f) del artículo 89 de la presente ley cuando se trate de una sanción exclusiva y dictaminar preceptivamente ante el Poder Ejecutivo para la adopción de las restantes.

V) Constituir, cuando corresponda, el Tribunal Arbitral que dirimirá en los conflictos entre partes, en el marco de lo establecido en los artículos 472 y siguientes del Código General del Proceso, procediéndose a la designación de los árbitros según lo dispuesto en el numeral 5) del artículo 3° de la Ley N° 16.832, de 17 de junio de 1997.

W) Convocar a audiencia pública cuando lo estime necesario, previa notificación a todas las partes interesadas, en los casos de procedimientos iniciados de oficio o a instancia de parte, relacionados con incumplimientos de los marcos regulatorios respectivos.

X) Asesorar preceptivamente al Poder Ejecutivo en materia de convenios internacionales u otros aspectos comprendidos en su competencia.

Y) Cumplir toda otra tarea que le sea cometida por la ley.

Si bien se realizaron algunos cambios respecto a las competencias anteriores que tenía la URSEC en el sector de telecomunicaciones, en general entiendo que se mantienen las competencias esenciales y que los cambios implementados, por un lado amplían las competencias en vista del fin buscado de fortalecer al Regulador, y por el otro lado, limitan la posibilidad de que el Poder Ejecutivo le otorgue competencias, restringiendo dicha posibilidad a la Ley, de conformidad a lo establecido en el artículo 190 de la Constitución.

(II.II.4) Administración Nacional de Telecomunicaciones (ANTEL) [134]

Se creó por medio del Decreto Ley Nº 14.235, como un servicio descentralizado, y con competencia, entre otras cosas, para prestar los servicios de telecomunicaciones

134 Véase nuestro trabajo ARAMENDÍA, MERCEDES, "Tipos de servicios de telecomunicaciones en el Uruguay y reglas de juego" en *Estudios de Telecomunicaciones y Sociedad de la Información,* Universidad de Montevideo, Montevideo, 2018, pp. 231 y ss.

urbanos y de larga distancia nacional e internacional (artículo 4 del Decreto Ley Nº 14.235).

El artículo 2 del Decreto Ley Nº 14.235 declara esenciales sus servicios, y el artículo 6º del mismo cuerpo normativo dispone que antel "*tendrá el monopolio de los servicios cuya prestación se le asigna por esta ley*".

Por medio de la Ley Nº 16.211 –Ley de Empresas Públicas– "*se modifica la carta orgánica de antel aprobada por Decreto-Ley Nº 14.235 y se deroga expresamente –por medio del Artículo 32– su monopolio o, más propiamente, su exclusividad (si se entiende que sus actividades participan de la naturaleza de servicio público)*"[135].

Posteriormente, en octubre de 1992 se realizó un Referéndum contra los artículos 1, 2, 3, 10 y 32 de la Ley de Empresas Públicas, estos artículos modificaban muchos aspectos de diferentes empresas públicas, entre esos cambios, se habilitaba a que antel fuera una sociedad de economía mixta y se derogaba el artículo 6 que establecía el monopolio de antel. Como consecuencia del Referéndum, los artículos que fueron objeto del mismo quedaron sin efecto en diciembre del mismo año.

Como enseña destacada doctrina "*En cuanto al monopolio de antel, se levantaron opiniones reivindicando su restablecimiento. Sin embargo, en rigor de Derecho, la derogación del Artículo 32º de la ley Nº 16.211 no pudo implicar la resurrección automática del derogado Artículo 6º de su carta orgánica puesto que si el legislador sanciona un precepto legal en el que se establece un determinado régimen jurídico, que luego es derogado por otra ley, y sobreviene un tercer acto –en el caso, el referéndum– que a su vez deroga esta última sin preceptuar que vuelva a regir la primera ley (lo cual no es posible por la vía del referéndum), el principio que domina la materia es que ésta no puede renacer porque no hay razones de lógica ni de técnica jurídica que así lo impongan*[136]*, según resulta de los precedentes nacionales relativos al caso en que el tercer acto derogatorio sea una ley. Corroborando lo expuesto, se ha reconocido que "la práctica administrativa se ha orientado en el sentido del no renacimiento de las*

135 DELPIAZZO, CARLOS, *Derecho de las Telecomunicaciones,* Universidad de Montevideo, 2005, pp. 30.

136 SUPERVIELLE, BERNARDO, "De la derogación de las leyes y demás normas jurídicas" en *Estudios Jurídicos en memoria de Juan José Amézaga,* Montevideo, 1958, pp. 495 y ss, citado por DELPIAZZO, CARLOS en obra citada, pp. 30 y ss.

normas derogadas y ello ha sido admitido tácitamente por todo el sistema político".[137, 138]

En el año 2001, por medio de los artículos 612 y 613 de la Ley Nº 17.296, se autorizaba a antel a constituir una sociedad anónima por acciones cuyo objeto fuera la prestación del servicio de telefonía celular terrestre, autorizándole a comercializar parte del paquete accionario[139], y se sustituían varios artículos de la carta orgánica de antel, entre estos: los Artículos 3 a 6, 8 a 10 y 12.

No obstante, como enseña el doctor Delpiazzo: *"Apenas aprobada la ley Nº 17.296, se inició un movimiento en su contra que se concretó en la interposición de un recurso de referéndum, en este caso contra los arts. 612 y 613.*

Ante tal circunstancia, se aprobó la ley Nº 17.524 de 5 de agosto de 2002, cuyo único objeto fue anticiparse a derogar expresamente ambas disposiciones, con lo que quedó sin objeto el referéndum"[140].

Al respecto como surge de la exposición de motivos que remitió el Poder Ejecutivo a la Asamblea General el 14 de mayo 2002, que finalizaría con la aprobación de la Ley N° 17.524: *"Es posición del Poder Ejecutivo que dado que estamos ante una discusión jurídica carente de sentido práctico y a los efectos de evitarle al país un costo por demás importante, resulta imprescindible dar por concluida la discusión proponiendo la derogación de los Artículos 612 y 613 de la Ley N° 17.296, de 21 de febrero, reiterando la ya admitida doctrina, en otro Artículo del proyecto de ley que el monopolio de antel solo resulta de aplicación para el caso de la telefonía básica,*

137 "A vía de ejemplo, en el caso de ILPE, cuando se derogó el Decreto-Ley Nº 15.370 de 11 de febrero de 1983, que era derogatorio del Decreto-Ley Nº 14.499 de 5 de marzo de 1976, se dispuso expresamente el restablecimiento de la plena vigencia de éste. De lo contrario, el mismo no habría podido renacer. Otro tanto acaba de ocurrir en el caso de la ley Nº 16.349 de 10 de abril 1993, la cual, al derogar el artículo 19 de la Ley Nº 15.737 de 8 de marzo de 1983, declaró "en vigor las normas que fueron derogadas expresa o tácitamente por la disposición citada", nota al pie realizada por DELPIAZZO, CARLOS en obra citada, pp. 32.

138 DELPIAZZO, CARLOS, *Derecho de las Telecomunicaciones*, Universidad de Montevideo, año 2005, pp. 32.

139 Interesante destacar que se establecía que el producido de la comercialización de dichas acciones se debía destinar a: A) Inversión en edificación escolar. B) Fomento de la actividad productiva utilizando la autorización existente a disminuir los tributos que la gravan por igual cantidad a las economías de los servicios de la deuda pública, que será cancelada con parte de los fondos. C) Inversión en Antel según disponga el Poder Ejecutivo.

140 DELPIAZZO, CARLOS, obra citada, pp. 36.

entendiendo por tal el servicio público de telefonía fija, conmutada y referida al tráfico nacional."

En esta línea, el proyecto de ley original disponía de dos artículos. El primero por medio del cual derogaba los artículos 612 y 613 de la Ley Nº 17.296, y el segundo que establecía lo siguiente: *"la prestación a terceros del servicio público de telefonía fija, conmutada y referida al tráfico nacional continuará siendo realizada en exclusividad por la Administración Nacional de Telecomunicaciones (antel)".*

Asimismo, el catedrático señala que respecto a la derogación del Artículo 613, en la medida que el mismo dispuso "*Sustituyénse los Artículos…"* podría entenderse que el efecto de la derogación es el restablecimiento de la vigencia de los textos sustituidos. En este sentido, si bien queda abierta la discusión respecto a la categorización jurídica de los servicios a cargo de antel, no cabe postular el renacimiento del monopolio previsto en el artículo 6º del Decreto-Ley Nº 14.235 por cuanto el mismo ya había sido derogado por el artículo 32 de la Ley Nº 16.211 –cuya derogación por referéndum no pudo rehabilitarlo–.[141]

En esta línea, el artículo 24 de la Ley N° 17.598 dispone que los servicios de telecomunicaciones y de postales, sujetos a la libre competencia, no pueden establecer regulaciones discriminatorias para los entes autónomos y servicios descentralizados del dominio industrial y comercial del Estado, que los coloquen en inferioridad de condiciones con respecto a sus competidores privados. Asimismo, se dispone que las regulaciones deben permitir la libre competencia en el mercado, evitando el abuso de la posición dominante, y que los cometidos sociales que, vinculados a distintas políticas, el Gobierno Nacional decida desarrollar a través de los entes o empresas del dominio industrial o comercial del Estado y cuyo cumplimiento implique pérdidas económicas, deben estar acompañados de los subsidios explícitos correspondientes para su financiamiento.

Finalmente, interesa comentar que en lo que respecta a si los servicios que presta antel son en régimen de competencia o de monopolio o de exclusividad, considerando:

1º que al Poder Ejecutivo corresponde ejecutar y hacer ejecutar las leyes;

141 DELPIAZZO, CARLOS, *Derecho Administrativo Especial*, Volumen 2, segunda edición, Amalio M. Fernández, 2009, pp. 225.

2º lo dispuesto por la Ley de Promoción y Defensa de la Competencia en cuanto dispone que todos los mercados están regidos por los principios y reglas de la libre competencia, excepto las limitaciones establecidas por ley por razones de interés general;

3º que la regla es la libertad y la excepción es la regulación;

4º que la actividad del Estado es la excepción, encontrándose sometido al principio de especialidad y debiendo regirse en su totalidad a lo dispuesto por el ordenamiento jurídico;

5º que nuestra Constitución admite la limitación de derechos, únicamente por razones de interés general que establezcan las leyes;

6º que el monopolio debe ser establecido conforme al artículo 85 numeral 17 de la Constitución por ley, por mayorías especiales;

7º que el artículo 6 del Decreto Ley N° 14.235 fue derogado por el artículo 32 de la Ley N° 16.211;

8º que como se reconoce en la Ley N° 17.598 los servicios de telecomunicaciones y postales tienen competidores privados;

9º que, como surge del artículo 2 de la Ley N° 17.820, en la redacción dada por el artículo 197 de la Ley N° 17.930 y el artículo 145 de la ley N° 18.046, el servicio de telefonía fija antel lo presta en condiciones de exclusividad;

Cabe concluir que la regla es la competencia, la excepción es la exclusividad (si se trata de servicio público) o el monopolio, y es manifiesto que el límite en la prestación no debería alcanzar más que el servicio de telefonía fija o básico.

En este sentido, vale subrayar que destacada doctrina ha sostenido: "*La telefonía de competencia de antel no constituye más servicio público; es actividad privada no monopolizada regida por el Derecho de la competencia*"[142].

142 DELPIAZZO, CARLOS, obra citada, citando a DURÁN MARTÍNEZ, AUGUSTO, "Competencia de ANTEL" en *Estudios de Derecho Público*, volumen I, Montevideo, 2004, pp. 235.; y PORRAS, BERNARDO, "La telefonía es actividad de libre competencia" en *Revista Tribuna del Abogado*, Nº 132, Colegio de Abogados del Uruguay, Montevideo, 2003, pp. 18 y ss.

(II.II.5) Prestadores de servicios privados

Para poder prestar los servicios de telecomunicaciones se requieren autorizaciones o licencias específicas otorgadas por el Poder Ejecutivo o la URSEC, según corresponda, en tanto si bien se tratan de actividades privadas, para poder prestar dichos servicios se requieren de actos administrativos, dictados por el Poder Ejecutivo, que expresamente lo autoricen.

Entre otras disposiciones, en lo que respecta a los servicios de telecomunicaciones, debemos tener presente lo establecido en el Reglamento de Licencias de Telecomunicaciones (RLT), aprobado por el Decreto Nº 115/003.

Vale destacar que nos encontramos ante actividad privada, de interés público, que se rige por el principio de libre y sana competencia, salvo las excepciones legalmente dispuestas.

Entre otras bases, el ordenamiento jurídico prevé que las licencias son por clases de servicios, disponen el alcance, los requisitos y las condiciones, así como los derechos y las obligaciones que se derivan de las mismas.

Cuando nos referimos a "*acto administrativo*", como dispone el artículo 120 del Decreto Nº 500/91, entendemos a toda manifestación de voluntad de la Administración que produce efectos jurídicos, y por "*autorización*", como enseña Sayagués, concebimos al acto administrativo que habilita a una determinada persona a ejercer un poder jurídico o derecho preexistente, que dependía de obtener previamente un acto de la administración que removiera el obstáculo jurídico y le habilitara a prestarlo.[143]

El RLT, aprobado por el Decreto N° 115/003, define en su artículo 3 a los "*Licenciatarios*", señalando que son las personas físicas o jurídicas a las cuales se les ha otorgado una autorización para la prestación de servicios de telecomunicaciones a terceros o al público en general; y a la "*Licencia*" como la autorización para la prestación de servicios de telecomunicaciones a terceros o al público en general.

Como ha entendido el Tribunal de lo Contencioso Administrativo[144], el término "licencia" está empleado como sinónimo de "autorización".

---

143 SAYAGUÉS LASO, ENRIQUE, *Tratado de Derecho Administrativo*, Tomo I, 9ª edición, Fundación de Cultura Universitaria, Montevideo, 2010, pp. 426.

144 Sentencia del TRIBUNAL DE LO CONTENCIOSO ADMINISTRATIVO N° 505/2015.

En esta línea, conforme se desprende del RLT, la "*licencia*" es la autorización para prestar servicios de telecomunicaciones a terceros o al público en general, dentro del área de servicio definida y en los términos establecidos en el acto administrativo correspondiente.

Vale señalar que la autorización para prestar los servicios, no supone la obligación del Poder Ejecutivo o de la URSEC de garantizar la disponibilidad de frecuencias o facilidades satelitales, lo cual en su caso se asignará de conformidad a su reglamentación específica.

Asimismo, se prevé la figura del revendedor de servicios de telecomunicaciones, el cual debe cumplir con las obligaciones atribuidas a los licenciatarios y estar inscripto en el registro de revendedores que lleva la URSEC.

En lo que respecta al contenido de la autorización o de la licencia, habrá que atender las condiciones que se establezcan en el acto administrativo correspondiente.

Vale destacar que, como se adelantó, entre los prestadores de servicios hay una empresa pública, la Administración Nacional de Telecomunicaciones (antel), que conforme a lo establecido en el Artículo 4º del Decreto-Ley 14.235, tiene entre sus competencias prestar los servicios de telecomunicaciones urbanos y de larga distancia, nacionales e internacionales.

El RLT,establece que las licencias son por clases de servicios[145]:

Clase A: *Habilita la operación de una red pública de telecomunicaciones y a la prestación por esos medios de los servicios de telecomunicaciones que resulten técnica y jurídicamente factibles conforme a la legislación vigente, con excepción del servicio de Televisión para abonados.*

Clase B: *Habilita la prestación de todos los servicios de transmisión de datos que resulten técnica y jurídicamente factibles conforme a la legislación vigente, utilizando como soporte la red, medios o enlaces propios o de otro prestador, en las condiciones que se pacten libremente entre las partes.*

145 Artículo 1 del Decreto 85/009 que modifica el artículo 9 del Reglamento de Licencias aprobado por el Decreto 115/003.

Clase C: *Habilita la instalación de enlaces, medios y sistemas de telecomunicaciones para su provisión o arriendo a licenciatarios de servicios de telecomunicaciones.*

Clase D: *Habilita la prestación de servicios de televisión por suscripción que requieren la utilización de medios de transmisión alámbricos o inalámbricos para la difusión de los contenidos*.

Como enseña el ingeniero Piaggio, "los operadores que tuvieran una licencia tipo A, son los de primera división en cuanto a recursos, inversión y control, y son los únicos que pueden operar una red pública de telecomunicaciones, con la consiguiente "supervisión" del Estado. Son los operadores fijo y móviles, los pldi, un operador de datos grande, etc. que tienen necesidad del uso de recursos escasos como la numeración tanto fija como móvil, recursos internacionales de identificación en telefonía tanto entrantes como salientes como son los dpc (Destination Point Code que es un numero finito y pequeño de códigos por país y que maneja la uit), etc. Estos operadores tienen privilegios (como *pedir más numeración) y responsabilidades como la obligación de interconectarse entre ellos (para que los clientes de unos puedan acceder a los clientes de otros operadores; sería un sin sentido que los operadores de uno de ellos solo pudieran hablar entre ellos y no pudieran llamar a otra personas que tuviera servicio con otro operador) con tecnologías fuertes, probadas, seguras, etc. y por lo tanto generalmente muy caras. Estos operadores tienen incluido la habilitaciones de las licencias tipo B y C, lo único que no pueden dar amparados en su licencia tipo A es el servicio de Televisión para Abonados (la Licencia tipo D).*"[146]

Asimismo, señala que: (i) la tipo B estaba pensada para operadores de datos, pequeños pldi, así como cualquier otro servicio de telecomunicaciones que fuera una red pública; (ii) la tipo C es para los carriers, brindan servicios al por mayor de capacidad en sus redes a otros operadores, no llegan al cliente final; y (iii) la tipo D es para los servicios de televisión por suscripción, por abonado, la cual se diferencia de la televisión abierta.

En la práctica, todas estas disposiciones han generado diversas interpretaciones y controversias, principalmente: (i) porque en los hechos solo antel presta servicios de

146 PIAGGIO, JUAN, "Nociones técnicas y prácticas de los servicios de telecomunicaciones en el país" en *Estudios de Telecomunicaciones y Sociedad de la Información,* Universidad de Montevideo, 2018, pp. 194.

transmisión de datos alámbricos, por más que se han presentado diversas solicitudes para poder prestar dichos servicios, el Poder Ejecutivo no les ha contestado o no los ha autorizado; (ii) por el alcance del principio de neutralidad tecnológico, que reconoce la libertad de los operadores de elegir la tecnología a través de la cual prestar los servicios; (iii) porque las licencias son por clases de servicios; (iv) por el principio de libre competencia; y (v) por el derecho de los usuarios de poder elegir.

Al respecto, como comentamos anteriormente, con el gran desarrollo que han tenido las telecomunicaciones, la convergencia y la Internet, el hecho de diferenciar las licencias por clases de servicios pierde cada vez más sentido, en tanto actualmente servicios completamente diferentes son prestados utilizando la misma red. De esta manera, ahora la prestación de un servicio no necesariamente debe estar relacionado con la provisión de una red. En tanto, la evolución tecnológica y de los mercados ha generado que las redes utilicen la tecnología de Internet (ip), al tiempo que los usuarios sustituyen los servicios tradicionales –como los mensajes de texto (sms) o la telefonía de voz– por servicios equivalentes pero que son prestados sobre la red ip, como por ejemplo voz sobre ip (voip). Al usuario final le es indiferente si el proveedor transporta él mismo la señal o si lo hace a través de un servicio de acceso a Internet. El medio que se utiliza es cada vez menos importante, en tanto ofrezca un rendimiento similar.[147]

En relación a los derechos y obligaciones de los prestadores en Uruguay[148], el RLT,prevé en su artículo 15 las obligaciones de los licenciatarios respecto a: (i) la prestación de los servicios, (ii) los usuarios, (iii) otros licenciatarios y (iv) específicamente para los que detentan una licencia clase A.

Respecto a la prestación de los servicios, los licenciatarios tienen las siguientes obligaciones:

i. Estar en condiciones de iniciar la prestación del servicio dentro del plazo de quince meses desde la fecha de obtención de la licencia, sin perjuicio de que pueda ser prorrogado por la URSEC por resolución fundada.

147 Exposición de Motivos Directiva (UE) 2018/1972 del Parlamento Europeo y de Consejo de 11 de diciembre de 2019, por la que se establece el Código Europeo de las Comunicaciones Electrónicas.

148 ARAMENDÍA, MERCEDES, obra citada, pp. 141 y ss.

ii. Cumplir el proyecto técnico presentado para la obtención de la licencia, en los términos en que fue aprobado por la URSEC.

iii. Suministrar a la URSEC toda la información requerida sobre la prestación de sus servicios.

Por otra parte, por Resolución N° 343/05 de URSEC se dispuso la implementación de la Base de Datos para uso regulatorio y el requerimiento de información a los operadores de servicios de telecomunicaciones y postales en carácter de declaración jurada. Posteriormente por medio de las resoluciones nros. 717/2009 y 427/2010 de URSEC, se realizaron modificaciones a los requerimientos establecidos por la Resolución N° 343/05. Actualmente se debe presentar información trimestralmente, con desagregación mensual, dentro de los primeros treinta días posteriores al vencimiento del trimestre para los servicios postales y de radiocomunicación, y dentro de los cuarenta y cinco días posteriores al vencimiento del trimestre que se informa para los servicios de televisión para abonados, telefonía móvil, telefonía de larga distancia internacional, telefonía fija y servicios de datos e Internet.

iv. Cumplir con las normas técnicas y los planes fundamentales elaborados y administrados por la URSEC.

v. Informar a la URSEC de cualquier falla mayor en el servicio.

En relación a las fallas, por Resolución Nº 96/2018, la URSEC aprobó el Reglamento de Calidad de Servicios y Experiencia de Clientes y Usuarios de Servicios de Telecomunicaciones (Reglamento de Calidad). En el artículo 9.2 de dicho Reglamento dispone lo vinculado a las interrupciones no programadas y señala que se considera falla masiva cuando se paralizan los servicios por un período igual o superior a 10 minutos y cuando afecte al 20 % o más de los clientes y usuarios.

En dichos supuestos, el operador debe informar a la URSEC de forma inmediata, por vía electrónica, lo siguiente:

a. identificación del suceso: lugar, instante de inicio, usuarios y/o clientes afectados, posibles causas, acciones correctoras en marcha y plazo previsible de solución;

b. durante el suceso: si se prolonga más del plazo previsto para su solución, deberá actualizar la información inicial, comunicar las medidas que se estén adoptando y aportar la información adicional que la URSEC le requiera;

c. al restablecimiento del servicio: informar la causa del problema, la solución del mismo y la hora exacta en que el servicio quedó disponible.

Asimismo, se prevé que en los casos en que haya interrupciones no programadas, por más de una hora, pero que no constituyan falla masiva; los operadores deben notificar a URSEC, por vía electrónica, dentro de los treinta minutos de haberse producido, en los mismos términos antes mencionada.

Finalmente, en el supuesto de que la interrupción no programada sea por causas de fuerza mayor o caso fortuito, los operadores dispondrán de un plazo de 10 días hábiles improrrogables para presentar a URSEC las pruebas que acrediten dicha circunstancia.

vi. Abonar los precios y tributos que surjan del marco regulatorio del sector.

En relación a las tasas, en el artículo 2° de la Ley N° 17.820, en la redacción dada por el Artículo 197 de la Ley N° 17.930 y por el artículo 145 de la ley N° 18.046, se creó la Tasa de Control del Marco Regulatorio (en adelante, tcmr), que se devengará por el control y la regularización de las actividades de telecomunicaciones y las referidas a la admisión, procesamiento, transporte y distribución de correspondencia realizada por operadores postales, así como por la entrega de envíos de correspondencia, giros postales y productos postales en general, de acuerdo a las leyes vigentes y a los convenios y acuerdos internacionales suscritos por la República.

La tcmr es equivalente al 3‰ (tres por mil) del total de ingresos brutos de la actividad sujeta a control, y debe destinarse, exclusivamente, a la financiación del presupuesto aprobado de la URSEC.

Las Resoluciones de URSEC números. 49/2007 y 194/2012 establecen los criterios para la presentación y pago de la tcmr. Se prevé que los operadores de servicios de comunicaciones deben declarar mensualmente los ingresos gravados por la tcmr en el sitio institucional de URSEC, teniendo carácter de declaración jurada, y se dispone que los operadores de servicios de telecomunicaciones y postales, tengan o no ingresos

gravados por la tcmr, deben presentar la declaración jurada dentro de los diez primeros días corridos siguientes al mes informado.

Asimismo, por Decreto N° 153/993, modificativo del Decreto N° 255/92, se aprueban las tasas y tarifas de los servicios administrados por la URSEC.

Por Decreto N° 332/013 se modificó el artículo 12 del Decreto N° 153/993, disponiendo que los valores en moneda nacional fijados en dicho Decreto se actualizan el 1º de enero de cada año, conforme a la evolución en el año inmediato anterior del Índice de Precios de Servicios de Comunicación y del Índice de Precios al Consumo (ipc), ambos publicados por el Instituto Nacional de Estadística (ine), ponderándose 85 % y 15 % respectivamente.

vii. Cumplir las normas y especificaciones técnicas en materia de equipos de telecomunicaciones y los requisitos técnicos que, en cada caso, resulten aplicables.

Al respecto se debe tener presente que, a fin de evitar interferencias perjudiciales a otros servicios y de garantizar un buen servicio, los equipo de telecomunicaciones que se encuentren en una de las siguientes categorías y que no sean expresamente exceptuados, deben ser homologados por URSEC. Hay dos tipos de homologaciones[149]:

a. Tipo I: equipos y aparatos de telecomunicaciones alámbricas destinados a conectarse directa o indirectamente a redes públicas de telecomunicaciones.

b. Tipo II: equipos de radiocomunicaciones.

viii. Cumplir con las metas de calidad y eficiencia que, en su caso, defina la URSEC para cada servicio.

Vale tener presente el Reglamento de Calidad, en el cual se determina, entre otras cosas, los niveles de calidad de servicios y de experiencia en la prestación de los servicios de telecomunicaciones, y se establecen métodos de medida. Los parámetros se pueden dividir en generales, que son de aplicación a todos los servicios, y específicos, que son de aplicación a servicios o al conjunto de servicios. En el caso de oferta conjunta de diferentes servicios de telecomunicaciones, los operadores deben tener en cuenta los parámetros de calidad asociados a cada servicio[150].

149 Artículo 20 del Reglamento de Licencias de Telecomunicaciones.
150 Resolución de URSEC Nº 96/2018.

Todos los operadores de servicios de telecomunicaciones deben comunicar a URSEC e informar a través de su página web y de sus servicios de atención al cliente, las condiciones de prestación del servicio, conforme a lo dispuesto en el Reglamento de Calidad. Asimismo, deben conservar los datos fuente, hasta transcurridos tres meses desde que se remitió la información, a fin de posibilitar el control y el seguimiento por parte de URSEC.

ix. Adoptar las medidas necesarias para asegurar el funcionamiento adecuado de sus instalaciones, no interferir a otros servicios, clientes o usuarios, garantizar la seguridad de los bienes y de las personas, y atender a los requerimientos en materia de defensa nacional y de seguridad pública que le sean formulados por las autoridades competentes.

Al respecto, interesa tener presente lo establecido en el artículo 20 de la Ley N° 18.331, en tanto establece que los operadores que exploten redes públicas o que presten servicios de comunicaciones electrónicas disponibles al público, deberán garantizar, en el ejercicio de su actividad, la protección de los datos personales. Asimismo, se indica que deberán adoptar las medidas técnicas y de gestiones adecuadas para preservar la seguridad en la explotación de su red o en la prestación de sus servicios, con el fin de garantizar sus niveles de protección de los datos personales que sean exigidos por la normativa. Lo anterior, es sin perjuicio de lo previsto en la normativa específica sobre telecomunicaciones, relacionadas con la seguridad pública y la defensa nacional.

En esta línea, interesa tener presente lo establecido en el Código del Proceso Penal, Ley N° 19.293, en los artículos 205, 206 y 207, en relación de la interceptación e incautación postal y electrónica, y los Artículos 208 y 209 respecto a la intervención de comunicaciones.

El Ministerio Público debe solicitar al tribunal competente la interceptación, incautación y ulterior apertura o registro de cualquier correspondencia, envío postal, correo electrónico o similar, dirigido al imputado o enviado por este aún bajo nombre supuesto, o de aquellos que le fueren atribuibles. Quedan excluidas las comunicaciones entre el imputado y su defensor. Se podrán dictar las mismas medidas respecto a terceros, si el juez tiene motivos seriamente fundados para suponer que de las mencionadas comunicaciones pudieran resultar prueba de la participación en un delito. Una vez recabada la autorización, el fiscal efectivizará la diligencia de interceptación e incautación. El fiscal será quien examine el contenido de la comunicación y si tiene

relación con la investigación, dispondrá su incautación dando cuenta al tribunal. Quien tenga en su poder la correspondencia requerida debe entregarla inmediatamente al fiscal, salvo que invoque causa legítima para no hacerlo, en cuyo caso se estará a lo que decida el tribunal.[151]

Respecto a la intervención, grabación o registro de comunicaciones telefónicas u otras formas de comunicación, cuando existan suficientes elementos de convicción para considerar que se ha cometido o pudiere cometerse un hecho punible, el fiscal podrá solicitar al juez la intervención y grabación de comunicaciones telefónicas, radiales o de otras formas de comunicación. El tribunal resolverá de forma inmediata, reservada y fundada, debiendo ponderar expresamente la necesidad y la proporcionalidad de la medida, bajo pena de nulidad. No se puede interceptar las comunicaciones entre el imputado y su defensor salvo que el tribunal lo ordene por estimar fundadamente que el abogado puede tener responsabilidad penal en los hechos investigados.[152]

La resolución judicial que disponga la interceptación deberá indicar: (i) nombre del afectado; (ii) de ser posible, línea telefónica u otro medio de comunicación a intervenir, grabar o registrar; (iii) forma, alcance y duración de la medida, no podrá exceder de seis meses; y (iv) autoridad o funcionario que se encargará de la diligencia.[153]

La medida cesará si los elementos considerados para ordenarla desaparecieran o si hubiera transcurrido el plazo de su duración.

La intervención de comunicaciones telefónicas, radiales o de otras formas de comunicación será registrada mediante su grabación magnetofónica u otros medios técnicos análogos, y el fiscal dispondrá la trascripción de la grabación, labrando el acta correspondiente, sin perjuicio de conservar el original.[154]

Asimismo, cabe tener presente lo establecido en el artículo 81 de la Ley Nº 19.670 que prevé la obligación de los operadores de servicios móviles de disponer de mecanismos que permitan identificar los aparatos de telefonía móviles a los que presten servicios; y lo dispuesto por el artículo 97 de la misma ley, que dispone que las

151 Artículos 205 a 207 del Código del Proceso Penal.
152 Artículos 208 del Código del Proceso Penal.
153 Artículos 208.4 del Código del Proceso Penal.
154 Artículos 209 del Código del Proceso Penal.

operadoras de telecomunicaciones, en las llamadas efectuadas a la emergencia 911 desde los servicios de telefonía móvil, deberán proporcionar al Ministerio del Interior, la localización geográfica del dispositivo al momento de la llamada, con la mayor precisión posible: radio base, celda celular, gps y demás datos que se obtengan de la misma, mediante los mecanismos técnicos que se especifiquen para recepción de los mismos.

x. Obtener autorización del Poder Ejecutivo o de la URSEC según corresponda, respecto de cualquier modificación de las participaciones accionarias en las sociedades titulares de licencias.

xi. Obtener autorización previa del Poder Ejecutivo o de la URSEC según corresponda, para la transferencia o cesión de la Licencia.

xii. Llevar contabilidad separada por servicios, en caso de que la URSEC así lo establezca con carácter general, respecto de determinados servicios o clase de Licencias.

Respecto de otros licenciatarios, tienen las siguientes obligaciones:

i. Respetar los principios de sana competencia y no incurrir en conductas anticompetitivas, conforme lo establecido en la legislación vigente.

Conforme al artículo 27 de la Ley Nº 18.159, a la URSEC le compete la protección y el fomento de la competencia en el sector. El objeto es "*fomentar el bienestar de los actuales y futuros consumidores y usuarios, a través de la promoción y defensa de la competencia, el estímulo a las eficiencia económica y la libertad e igualdad de condiciones de acceso de empresas y productos a los mercados*"[155]. Se establece como principio general que "*Todos los mercados estarán regidos por los principios y reglas de la libre competencia, excepto las limitaciones establecidas por ley, por razones de interés general*[156]". En esta línea, "*prohíbe el abuso de posición dominante, así como todas las prácticas, conductas o recomendaciones, individuales y concertadas, que tengan por efecto u objeto, restringir, limitar, obstaculizar, distorsionar o impedir la competencia actual o futura en el mercado relevante*"[157]. En lo que respecta al ámbito subjetivo[158], están obligadas a regirse por los principios de la libre competencia todas las personas físicas y jurídicas, públicas y privadas, nacionales

155 Artículo 1º de la Ley Nº 18.159.
156 Artículo 2 de la Ley Nº 18.159.
157 Ibídem.
158 Artículo 3 de la Ley Nº 18.159.

y extranjeras, que desarrollen actividades económicas con o sin fines de lucro en el territorio uruguayo.

ii. Proveer interconexión o acceso a los recursos de numeración, señalización, enlaces u otros medios de las Redes Públicas de Telecomunicaciones en los casos que corresponda, según la normativa vigente.

Finalmente, respecto de los clientes o usuarios, los licenciatarios tienen las siguientes obligaciones:

i. Dar a los clientes o usuarios información adecuada y veraz respecto de las condiciones de prestación y de contratación de los servicios.

ii. Hacer públicos los precios, promociones y planes de los servicios ofrecidos.

iii. No incluir en los contratos de servicios con los clientes, cláusulas que impliquen desequilibrios injustificados entre los derechos y obligaciones de las Partes.

iv. Diseñar las facturas de forma que la información sea fácil de entender y los conceptos a pagar ampliamente discriminados, por ejemplo según: servicios, segmentos horarios, abono, cargos fijos, cargos variables, servicios suplementarios, carga impositiva, etc.

v. Habilitar un número telefónico para que los clientes puedan acceder a información sobre los servicios y puedan efectuar reclamos.

vi. Instalar centros de atención al cliente en las capitales departamentales del país en las que presten servicios. En dichos centros, tiene que haber personal suficiente para brindar atención personalizada, y además se debe difundir: la ubicación de los centros, el número de teléfono, facsímil y el horario de atención.[159]

Más allá de lo anterior, a los titulares de Licencia de Telecomunicaciones Clase A se les establecen obligaciones adicionales, como ser:

i. Adoptar medidas para que la red pueda incorporar nuevos servicios, funciones y facilidades.

159 Artículo 1 del Decreto 83/013.

ii. Cumplir con el Reglamento de Interconexión y Sistema Multiprestador de Larga Distancia, así como adecuar su red a los requerimientos establecidos en los Planes Técnicos Fundamentales actuales y futuros.

Por otra parte, en lo que respecta a los revendedores de servicios de telecomunicaciones, como se mencionó anteriormente, los mismos además de cumplir con las obligaciones atribuidas a los licenciatarios, también deben estar inscriptos en el registro de revendedores que lleva la URSEC. Los revendedores tienen responsabilidad directa ante el cliente final por los servicios que comercializan y por las condiciones de calidad, confiabilidad y precio; están obligados a hacer públicos sus tarifas, promociones, planes ofrecidos y a abonar todos los precios y tributos que en su caso correspondan.

En contraposición de las obligaciones señaladas, se puede concluir que los prestadores tienen, entre otros, los siguientes derechos:

1. A prestar sus servicios en los términos y condiciones dispuestos.

2. A ser elegidos por todo cliente.

3. A que se promueva y defienda la libre competencia, la eficiencia económica, la libertad e igualdad de condiciones de acceso de empresas y productos a los mercados.

4. A que se promuevan y defiendan las inversiones, otorgando igualdad y tratamiento justo[160].

5. A acceder a Interconexión, acordando el precio y las condiciones, en condiciones no discriminatorias.

6. A obtener condiciones equivalentes a las que se estén otorgando a otros prestadores en similares circunstancias.

7. A acceder a los recursos de numeración, señalización y enlaces.

8. A acceder de forma equitativa a recursos radioeléctricos, conforme a lo establecido en el Reglamento de Administración del Espectro Radioeléctrico y en la legislación nacional.

160 Ley N° 16.906.

9. A usar las frecuencias del espectro radioeléctrico que le hayan sido asignadas.

10. A elegir la tecnología a través de la cual prestar sus servicios.

11. A desplegar redes/infraestructura para la prestación de sus servicios. En relación a este punto interesa destacar el Decreto-Ley N° 14.442 el cual dispone en su Artículo 1°: *"Queda sujeto a la servidumbre respectiva, con carácter gratuito, para servicio de Telecomunicaciones, todo edificio sobre el cual sea necesario fijar líneas, cables, soportes de antenas para equipos radioeléctricos y canalizaciones especiales. Quedan sujetos a la misma servidumbre y para instalaciones subterráneas las calles, plazas, caminos y terrenos de las zonas urbanas, suburbanas y Rurales".*

(III) Bases de la Regulación en España

El marco normativo español en relación a las telecomunicaciones es mucho más amplio, desarrollado y actualizado que el de Uruguay.

Además de tener que transponer a su ordenamiento el marco regulador de las comunicaciones electrónicas aprobado por la Unión Europea, cuenta con disposiciones constitucionales que reconocen a las comunicaciones dentro de los derechos fundamentales.

Específicamente el Título I "*De los derechos y deberes fundamentales*", capítulo segundo "*Derechos y Libertades*", sección 1º "*De los derechos fundamentales y de las libertades públicas*", en el artículo 18.3 se dispone que: "*3. Se garantiza el secreto de las comunicaciones, y en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial*", y el artículo 18.4 se señala que: "*4. La ley limitará 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".*

Asimismo, en el Título VIII: *"De la organización Territorial del Estado"*, capítulo tercero: "*De las Comunidad Autónomas*", se dispone que: "*1. El Estado tiene competencia exclusiva sobre las siguientes materias:*

1º. La regulación de las condiciones básicas que garanticen la igualdad de todos los españoles en el ejercicio de los derechos y en el cumplimiento de los deberes constitucionales. (...)

13º. Bases y coordinación de la planificación general de la actividad económica. (...)

21º. Ferrocarriles y transportes terrestres que trascurran por el territorio de más de una Comunidad Autónoma; región general de comunicaciones; tráfico y circulación de vehículos a motor; correos y telecomunicaciones; cables aéreos, submarinos y radiocomunicación."

En el año 2003 se dictó la Ley General de Telecomunicaciones Nº 32/2003, por medio de la cual se transpuso el marco regulador de las comunicaciones electrónicas aprobado por la Unión Europea del año 2002. Desde entonces la Ley General se ha ido modificando a efectos de adecuarse a la nueva realidad y a los requerimientos.

La Ley vigente, Nº 9/2014 (LGT), persiguió los objetivos de la Agenda Digital europea al 2020, buscando generar un marco regulatorio que fuera claro y establece, a fin de facilitar la inversión, dar seguridad, eliminar las barreras que dificultan el despliegue de redes y promover la competencia.

En base a las disposiciones constitucionales antes mencionadas y a la normativa de europea, se buscó: (i) recuperar la unidad del mercado, (ii) coordinar el sector y resolver conflictos, (iii) facilitar el despliegue y la prestación de servicios, (iv) simplificar, eliminando licencias y autorizaciones para determinadas categorías, (v) promover la competencia, (vi) racionalizar el gasto, (vii) se incorpora a la Comisión Nacional de los Mercados y de la Competencia, creada por la Ley 3/2013, atribuyéndole competencia de regulación ex ante y de resolución de conflictos, (viii) reducir las cargas y obligaciones, y (ix) reforzar el control del espectro radioeléctrico.

En definitiva, la norma está inspirada en los criterios de: (i) liberalización del sector, (ii) libre competencia, (iii) recuperación de la unidad de mercado, y (iv) reducción de cargas. A fin de generar las condiciones necesarias para el crecimiento económico del país, como son: (i) seguridad jurídica, (ii) competencia efectiva, (iii) inversiones en el despliegue de redes y de servicios de última generación.

La Ley General de Telecomunicaciones (LGT) atiende específicamente la regulación de las telecomunicaciones, adoptando la misma definición dispuesta en el Convenio Internacional de Telecomunicaciones de 1973 : *"toda transmisión, emisión o recepción de signos, señales, escritos o imágenes, sonidos o informaciones de cualquier naturaleza por hilo, radioelectricidad, medios ópticos u otros sistemas*

electromagnéticos[161]*¨;* comprendiendo la explotación de redes y la prestación de los servicios de comunicación electrónica, así como los recursos asociados. Excluye a los servicios de comunicaciones audiovisual, los contenidos audiovisuales transmitidos a través de las redes, así como los medios de comunicación social de naturaleza audiovisual[162]. Así como a los servicios que suministres contenidos a través de redes y de servicios de comunicaciones electrónicas, el control editorial de los contenidos y los servicios de la Sociedad de la Información, los cuales están regulados por la Ley Nº 34/2002.

Se parte de la base de que las telecomunicaciones son servicios de interés general y que se prestan en régimen de libre competencia[163]. No son servicios públicos. Solo se consideran que tienen dicha calidad los servicios de telecomunicaciones para la defensa nacional, la seguridad pública, la seguridad vial y la protección civil (artículo 4 de la Ley Nº 9/2014).

(III.I) Objeto y fin de la prestación de los servicios de telecomunicaciones en España.

Las telecomunicaciones son servicios de interés general que se prestan en régimen de libre competencia.

Conforme a lo establecido en el artículo 3 de la LGT, los objetivos y principios en los que se basa son los siguientes:

a) Fomentar la competencia efectiva para potenciar los beneficios para las empresas y los consumidores, especialmente mejorando la accesibilidad, en tanto bajan los precios los precios y aumenta la calidad de los servicios y la innovación.

b) Desarrollar la economía y el empleo digital, a través de la promoción del sector de las telecomunicaciones y de todos los nuevos servicios, impulsando la integración social y territorial.

c) Promover el despliegue de redes y la prestación de servicios de comunicaciones electrónicas, para lo cual se fomenta la conectividad, la interoperabilidad y el acceso.

d) Impulsar la industria de productos y equipos de telecomunicaciones.

---

[161] Anexo II de la Ley 9/2014, General de Telecomunicaciones de España, punto 39.
[162] Artículo 1, inciso 2, de la Ley Nº 9/2014, General de Telecomunicaciones de España.
[163] Artículo 2, inciso 1, de la Ley Nº 9/2014, General de Telecomunicaciones de España.

e) Contribuir con el crecimiento del mercado de servicios de comunicaciones electrónicas.

f) Promover la inversión eficiente de infraestructuras, fomentando la innovación y mitigando los riesgos.

g) Utilizar de forma eficaz los recursos de telecomunicaciones, por ejemplo: numeración y el espectro radioeléctrico.

h) Fomentar la neutralidad tecnológica.

i) Garantizar las obligaciones de servicio público, en especial las de servicio universal.

j) Defender a los usuarios, asegurando el acceso a servicios de buen precio y calidad, pudiendo elegir y promoviendo el desarrollo de capacidades por parte de los usuarios para acceder, utilizar los servicios y aplicaciones, y distribuir la información. Se deben proteger los derechos fundamentales, como son: no discriminación, respeto al honor y a la intimidad, protección a la juventud y a la infancia, el secreto de las comunicaciones y la protección de los datos personales.

k) Atender los principios de oportunidad y no discriminación, salvaguardando las necesidades y facilitando el acceso a los servicios a grupos sociales específicos, como pueden ser las personas con discapacidad, mayores o usuarios con necesidades especiales.

En lo que respecta a los principios que rigen la explotación y la prestación de los servicios, el artículo 5 de la LGT, dispone que se rigen por la libre competencia, más allá de limitaciones que se establecieren en la propia Ley y por la normativa que la desarrolle.

Para acceder a los derechos de uso de bienes limitados, como puede ser, ocupar dominio público, acceder a numeración, a espectro radioeléctrico, así como a otros elementos necesarios para prestar servicios de comunicaciones electrónicas, se deberá regir por lo establecido por la LGT, debiendo atender también lo que se disponga en la normativa específica.

Todas las medidas que se adopten deben estar en línea con lo establecido en el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades

Fundamentales, en la Carta de Derechos Fundamentales de la Unión Europea, en los principios generales del Derecho comunitario y en la Constitución Española.

Cualquier limitación relativa al acceso o al uso de los servicios, solo podrá establecerse siempre que sea adecuada, proporcionada y necesaria, debiendo seguir los procedimientos apropiados para garantizar debidamente los derechos y libertades, respetando la presunción de inocencia, la vida privada, estableciendo procedimientos justos, imparciales y justo, teniendo el interesado el derecho a ser oído, a la tutela judicial efectiva y que se realice en tiempo oportuno.

En relación al acceso a las redes, a los recursos asociados y a la interconexión, el artículo 12 de la LGT prevé que los operadores de redes públicas de comunicaciones electrónicas tienen el derecho y el deber de negociar la interconexión mutua para prestar los servicios, a fin de garantizar la prestación de los servicios y la interoperabilidad.

En aquellos casos en que una de las empresas tenga un poder significativo en el mercado, la Comisión Nacional de los Mercados y la Competencia (CNMC) puede intervenir, de oficio o a petición de alguna de las partes, para fomentar y garantizar el acceso, la interconexión y la interoperabilidad de los servicios.

Las medidas que se adopten deben ser: transparentes, proporcionales, objetivas y no discriminatorias.

La información que se deba compartir en el proceso de negociación, solo podrá ser utilizada para los fines para los que fue facilitada, respetando la confidencialidad.

A fin de que los servicios de comunicaciones electrónicas puedan ser prestados al público, se proporcionará números, direcciones y nombres que sean necesarios.

El Gobierno debe aprobar los planes nacionales de numeración, de direccionamiento y de denominación, para lo cual debe considerar las medidas adoptadas en organizaciones y foros internacionales. Para lo cual el Ministerio de Industria, Energía y Turismo (MIET) debe remitir propuestas, así como desarrollar la normativa necesaria para dichos planes.

Aprobados los planes nacionales, el MIET es quien debe otorgar los derechos de uso de los recursos públicos, ateniendo procedimientos dispuestos por Real Decreto que deberán ser abiertos, objetivos, no discriminatorios, proporcionales y transparentes.

Interesa destacar que los operadores que detenten el derecho de usar una serie de números, no pueden discriminar a otros operadores para dar acceso a los servicios.

Las decisiones adoptadas por el MIET en materia de numeración, direccionamiento y denominación, serán obligatorias para todos los operadores, fabricantes y comerciantes.

En esta línea, siempre que sea técnica y económicamente posible, los operadores que exploten redes públicas de comunicaciones o presten servicios telefónicos disponibles al público, deben adoptar las medidas necesarias para que los usuarios finales puedan tener acceso a los servicios, a todos los números proporcionados en la Unión Europea, los del espacio europeo de numeración telefónica, y los Números Universales Internacionales de Llamada Gratuita.

Se quieren garantizar servicios de comunicaciones electrónicas de calidad, al público, en todo el territorio nacional, a través de la competencia y de la posibilidad de poder elegir.

Para la prestación de los servicios y la explotación de las redes, se deberán respetar los principios de igualdad, transparencia, no discriminación, continuidad, adaptabilidad, disponibilidad y permanencia y la normativa aplicable.

Para la prestación de los servicios y el uso del espectro radioeléctrico, se podrá emplear cualquier tipo de tecnología, conforme al principio de neutralidad tecnológica. Sin perjuicio, se podrán establecer restricciones proporcionales y no discriminatorias, en caso de ser necesarios para evitar interferencias perjudiciales, proteger la salud pública, asegurar la calidad técnica de los servicios, garantizar el uso compartido y eficiente de las frecuencias radioeléctricas, así como para alcanzar objetivos de interés general.

En esta línea, conforme a lo establecido en el Cuadro Nacional de Atribución de Frecuencias, en las bandas declaradas para los servicios de comunicaciones electrónicas, se podrá prestar cualquier tipo de servicio de comunicaciones. Sin perjuicio, se podrán establecer restricciones a los tipos de servicios a prestar, siempre que sean proporcionales y no discriminatorias. Asimismo, se podrá exigir que determinados servicios se presten en bandas específicas para garantizar alcanzar objetivos de interés general establecidos en el Derecho de la Unión Europea, como pueden ser: asegurar la vida, promover la cohesión social, regional o territorial, evitar el uso ineficiente del

espectro radioeléctrico, promover la diversidad cultural, lingüística y el pluralismo de los medios de comunicación.

Interesa destacar que cuando la prestación del servicio universal no esté garantizada por el libre mercado, el MIET va a designar a uno o más operadores para garantizar la prestación eficiente, de manera que quede cubierto todo el territorio nacional. La forma se va a establecer por real decreto, atendiendo los principios de eficiencia, objetividad, transparencia y no discriminación, buscando que se haga de forma rentable.

En relación a la protección del dominio público radioeléctrico, lo que se busca es que se pueda aprovechar de forma óptima, evitando la degradación y ofreciendo un nivel de calidad adecuado en el funcionamiento de los servicios.

Se busca garantizar el uso eficaz y eficiente del espectro radioeléctrico, la neutralidad tecnológica de los servicios y también en el mercado secundario[164], así como fomentar la competencia.

Sin perjuicio, se prevé que se pueda limitar la propiedad, la intensidad de los campos electromagnéticos y las servidumbres necesarias para proteger las instalaciones y asegurar el funcionamiento, para la seguridad pública y cuando se requiera por acuerdos internacionales.

Cuando las administraciones públicas dicten normativas que puedan afectar el despliegue de redes de comunicaciones electrónicas, así como los instrumentos de planificación territorial, deben atender la normativa de telecomunicaciones, especialmente los parámetros y requerimientos técnicos para garantizar el funcionamiento de las redes y de los servicios, y los límites de emisión radioeléctrica tolerables. En estos casos, las administraciones deben actuar conforme a los principios de necesidad, proporcionalidad, seguridad jurídicas, transparencia, accesibilidad, simplicidad y eficacia.

[164] Está regulado en el Título VI del Real Decreto 123/2017. El objeto es flexibilizar el uso y hacerlo más eficiente. Los negocios jurídicos relativos al mercado secundario q se prevén son: (i) la transferencia de títulos habilitantes para el uso privativo de ER,(ii) la cesión de derecho de uso privativo del ER,(iii) la mutualización de los derechos de uso privativo del ER,y (iv) la provisión de servicios mayoristas. Cualquiera de estos negocios jurídicos debe ser autorizado previamente por el Ministerio de Energía, Turismo y Agenda Digital o por la Secretaría de Estado para la Sociedad de la Información y la Agenda Digital, según corresponda. De lo contrario, será nulo de pleno derecho y se tendrá por no celebrado.

(III.II) Diseño Institucional

Se establece competencia de diversas autoridades nacionales, las cuales en el cumplimiento de sus cometidos deben atender principios regulatorios como son: objetividad, transparencia, no discriminación y proporcionalidad, a fin de garantizar:

- Entorno regulador previsible, coherente y que se revide en períodos apropiados.
- Fomentar la inversión en innovación, en infraestructura, teniendo en cuenta los riesgos que asumen los inversores, permitiendo la cooperación, buscando diversificar el riesgo, respetar la competencia y la no discriminación.
- Competencia efectiva y sostenible, estableciendo obligaciones ex ante solo cuando se afecte dicha competencia, debiendo eliminarse en cuanto haya cumplimiento.
- Trato igualitario, no discriminatorio, entre las empresas prestadores de redes y servicios.
- La competencia beneficia a los consumidores y a los proveedores, cuando se posible promoverla en las infraestructuras.
- Tener en cuenta la variedad de condiciones en las distintas regiones geográficas.
- Promover la eficiencia, la competencia sostenible y buscar el máximo beneficio para los usuarios finales.

Se consideran "Autoridad Nacional de Reglamentación de Telecomunicaciones": (i) al Gobierno, (ii) a los órganos superiores y directivos del Ministerio de Industria, Energía y Turismo que asuman competencias asignadas a dicho ministerio en relación a esta materia, (iii) a los órganos superiores y directivos del Ministerio de Economía y Competitividad que asuman competencias asignadas a dicho ministerio en relación a esta materia, y (iv) la Comisión Nacional de los Mercados y la Competencia (CNMC) en las competencias que se le asignen en la materia.

Los diversos organismos deberán cooperar entre sí, así como con los demás órganos de control de otros Estados y de la Unión Europea, a fin de promover la aplicación coherente de la normativa comunitaria. Debiendo apoyar activamente a la

Comisión y del Organismo de Reguladores Europeos de las Comunicaciones Electrónicas (ORECE), colaborando para determinar los instrumentos y las soluciones más adecuados para el mercado.

(III.II.1) El Ministerio de Industria, Energía y Turismo (MIET).

Conforme lo establecido en el artículo 69 de la LGT, en línea con la estructura orgánica del departamento, los órganos superiores y directivos del MIET, en relación a los servicios de telecomunicaciones deben ejercer las siguientes funciones:

a) Ejecutar las políticas que sean adoptadas por el Gobierno.

b) Gestionar el Registro de Operadores.

c) Ejercer las competencias que le atribuya la LGT y su desarrollo reglamentario, en especial los siguientes: (1) procedimientos de licitación para la obtención de derechos de uso del dominio público radioeléctrico; (2) garantizar el cumplimiento de las normas relativas a la protección de los datos personales y a la intimidad de las personas; y (3) cumplir compromisos internacionales en la materia.

d) Proponer al Gobierno: (i) la aprobación de los planes nacionales de numeración, direccionamiento y denominación; (ii) la política a seguir para facilitar el desarrollo y la evolución de las obligaciones de servicio público; (iii) la política para reconocer y garantizar los derechos y obligaciones en la explotación de las redes y en la prestación de los servicios, así como garantizar los derechos de los usuarios finales.

e) Otorgar los derechos de uso de los recursos pública de numeración, direccionamiento y denominación.

f) Controlar y seguir el cumplimiento de las obligaciones de servicio público que correspondan a los distintos operadores.

g) Gestionar el Registro de empresas instaladoras de telecomunicación.

h) Formular propuestas para elaborar la normativa relativa a las infraestructuras comunes de comunicaciones electrónicas en el interior de edificios y conjuntos inmobiliarios, y el seguimiento de su implantación.

i) Evaluar la conformidad de equipos y aparatos.

j) Administrar el espectro radioeléctrico, en especial: (i) planificar, gestionar y controlar el dominio público radioeléctrico, (ii) así como la tramitación y el

otorgamiento de las habilitaciones para su utilización, (iii) autorización e inspección de instalaciones radioeléctricas en relación con los niveles únicos de emisión radioeléctrica, (iv) gestión de un registro público de radiofrecuencias, accesible a través de Internet, (v) elaborar proyectos y desarrollar planes técnicos nacionales de radiodifusión y televisión, (vi) comprobar técnicamente las emisiones radioeléctricas para la identificación, localización y eliminación de interferencias perjudiciales, infracciones, irregularidades y perturbaciones de los sistemas de radiocomunicación, (vi) verificar el uso efectivo y eficiente del dominio público radioeléctrico por parte de los titulares de derechos de uso, (vii) proteger el dominio público radioeléctrico, para lo cual podrá realizar emisiones en aquellas frecuencias y canales radioeléctricos cuyos derechos de uso, en el ámbito territorial correspondiente, no hayan sido otorgados, (viii) gestionar la asignación de los recursos órbita-espectro para comunicaciones por satélite, (ix) elaborar estudios e informes y asesorar a la Administración General del Estado en todo lo relativo a la administración del dominio público radioeléctrico, (x) participar en los organismos internacionales relacionados con la planificación del espectro radioeléctrico.

k) Gestionar en período voluntario las tasas en materia de telecomunicaciones.

l) Gestionar, liquidar, inspeccionar y recaudar las aportaciones a realizar por los operadores de telecomunicaciones y por los prestadores privados del servicio de comunicación audiovisual televisiva, de ámbito geográfico estatal o superior al de una Comunidad Autónoma.

m) Realizar cualesquiera otras funciones que expresamente se le atribuidas por normativa comunitaria, LGT y por su normativa de desarrollo, o por real decreto.

El MIET fomentará el uso de normas o especificaciones técnicas en línea con las determinadas por la Comisión Europea para armonizar el suministro de redes y la prestación de los servicios, en especial garantizará la aplicación de aquellas que se establezcan como obligatorias, para la interoperabilidad y potenciar la libertad de elegir de los usuarios. En ausencia de dichas normas, promoverá la aplicación de las normas aprobadas por la Unión Internacional de Telecomunicaciones (UIT), la Conferencia Europea de Administraciones de Correos y Telecomunicaciones (CEPT), la Comisión

Internacional de Normalización (ISO) y la Comisión Electrotécnica Internacional (CEI).[165]

Por otra parte, al MIET le compete la inspección de: (a) las condiciones de prestación y de explotación de los servicios y de las redes de comunicaciones electrónicas; (b) la instalación y de los sistemas de de los equipos y aparatos; (c) el dominio público radioeléctrico; y (d) los servicios de tarificación adicional que se soporten sobre redes y servicios de comunicaciones electrónicas[166].

Al Secretario de Estado de Telecomunicaciones y para la Sociedad de la Información, para la imposición de sanciones no contempladas en los siguientes apartados.

Salvo las que le competen a la CNMC y a la Agencia Española de Protección de Datos[167].

(III.II.2) La Comisión Nacional de los Mercados y la Competencia (CNMC).

La LGT se remite a la Ley de Creación de la CNMC en lo que respecta a su naturaleza, funciones, estructura, personal, presupuesto y demás elementos[168].

En relación a la materia se ocupa, conforme a lo establecido en el artículo 70 de la LGT, le compete:

---

[165] Artículo 11 de la LGT.
[166] Artículo 72 de la LGT.
[167] Conforme a lo previsto en la Ley 3/2018 de Protección de Datos Personales y garantías de los derechos digitales, la Agencia Española de Protección de Datos es una autoridad administrativa, con personalidad jurídica, con plena capacidad pública y privada, que actúa con plena independencia en el ejercicio de sus funciones y que se relaciona con el Gobierno a través del Ministerio de Justicia. Es la representante común de las autoridades de protección de datos de España en el Comité Europeo de Protección de Datos.

[168] Organismo público, independiente, sometida a control parlamentario, que promueve y defiende el buen funcionamiento de todos los mercados en interés de los consumidores y de las empresas. Se creó en el 2013 tras la integración de seis organismos: Comisión Nacional de la Competencia, Comisión Nacional de Energía, Comisión del Mercado de las Telecomunicaciones, Comisión Nacional del Sector Postal, Consejo Estatal de Medios Audiovisuales y Comité de Regulación Ferroviaria y Aeroportuaria. La aparición de esta pluralidad de organismos reguladores fue consecuencia de la liberalización de los mercados y la necesidad de adaptar la normativa económica española a la europea. Entre sus principales funciones: (i) aplicación de la normativa de defensa de la competencia española y la UE, (ii) promoción de la competencia, (iii) unidad de mercado, (iv) resolución de conflictos entre operadores económicos, y (v) supervisión y control de todos los sectores económicos – gas y electricidad, comunicaciones electrónicas y audiovisuales, ferroviario y aeroportuario, mercado postal-. Fuente: https://www.cnmc.es/sobre-la-cnmc/que-es-la-cnmc. Consultado el 16 de junio de 2019.

a) Definir y analizar los mercados relativos a redes y servicios de comunicaciones electrónicas, al por mayor y al por menor, y el ámbito geográfico de los mismos.

b) Cuando no se desarrolle un entorno de competencia efectivo, debe identificar al operador o a los operadores que detenten poder significativo en el mercado.

c) En su caso, establecer las obligaciones específicas para los operadores con poder significativo en mercados de referencia.

d) Resolver conflictos entre operadores en relación a: (i) la utilización compartida del dominio público o la propiedad privada, (ii) la ubicación compartida de infraestructuras y recursos asociados, (iii) el acceso a infraestructuras capaces de alojar redes públicas de comunicaciones electrónicas y, (iv) el acceso a las redes de comunicaciones electrónicas titularidad de los órganos o entes gestores de infraestructuras de transporte de competencia estatal.

e) Decidir la obligación de separación funcional a los operadores con poder significativo en el mercado integrados verticalmente.

f) Fijar las características y condiciones para la conservación de los números.

g) Fomentar y garantizar la adecuación del acceso, la interconexión y la interoperabilidad de los servicios, para lo cual puede intervenir en las relaciones entre operadores o entre operadores y otras entidades.

h) Determinar la cuantía que supone el coste neto en la prestación del servicio universal, así como definir y revisar la metodología para la determinación, la cual debe basarse en procedimientos y criterios objetivos, transparentes, no discriminatorios, proporcionales y ser de carácter público.

j) Establecer el procedimiento para cuantificar los beneficios no monetarios obtenidos por el operador u operadores encargados de la prestación del servicio universal.

k) Facilitar el acceso a programa de aplicaciones (API) y a guías electrónicas de programación (EPG), decidiendo en su caso la imposición de obligaciones a los operadores que dispongan de interfaces, si fuera necesario para garantizar el acceso a servicios digitales de radiodifusión y televisión.

l) Ser consultada por el Gobierno, el Ministerio de Industria, Energía y Turismo, las comunidades autónomas y las corporaciones locales en materia de comunicaciones electrónicas que puedan afectar al desarrollo libre y competitivo del mercado.

m) Participar, por medio de informe, en la elaboración de normas que afecten su ámbito de competencia.

n) Realizar arbitrajes, de derecho o de equidad, que le sean sometidas por los operadores de comunicaciones.

o) Realizar cualesquiera otras funciones que le sean atribuidas de manera expresa por la normativa comunitaria, la LGT, su normativa de desarrollo, por otra ley o por real decreto.

Por otra parte, fomentará el uso de normas o especificaciones técnicas en el ejercicio de la regulación ex ante y de resolución de conflictos[169]; al tiempo que se encarga de gestionar el Fondo Nacional de Servicio Universal[170].

Asimismo, le compete a la CNMC la inspección de las actividades de los operadores de telecomunicaciones respecto de las cuales tenga competencia sancionadora, pudiendo solicitar la actuación del Ministerio de Industria, Energía y Turismo[171].

En esta línea, cuando se trate de infracciones muy graves, expresamente tipificadas en os apartados 12, 15 y 16 del artículo 76 de la LGT, infracciones graves tipificadas en los apartados 11, 27, 28, 35 y 36 del artículo 77 de la LGT e infracciones leves tipificadas en el apartado 4 del artículo 78 de la LGT tiene competencia sancionadora.

(III.II.3) Prestadores de servicios.

Como surge del artículo 5 de la LGT, la explotación de las redes y la prestación de los servicios de comunicaciones electrónicas es en régimen de libre competencia, sin perjuicio de las limitaciones que establezcan en la LGT.

Para adquirir los derechos de uso del espectro radioeléctrico, de ocupación del dominio público o de la propiedad privada, así como de los recursos de numeración,

[169] Artículo 11.2 de la LGT.
[170] Artículo 27 de la LGT.
[171] Artículo 72 de la LGT.

direccionamiento y denominación, se debe atender lo establecido en la LGT y en su normativa específica.

En relación al acceso a los servicios por parte de los usuarios finales, se deben respetar los derechos y libertades fundamentales, conforme lo establecido en el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertad Fundamentales, en la Carta de Derechos Fundamentales de la Unión Europea, u en los principios generales del Derecho Comunitario y en la Constitución de España.

Pueden explotar redes y prestar los servicios a terceros, personas físicas o jurídicas de un Estado miembro de la Unión Europea o de otra nacionalidad, cuando esté previsto en acuerdos internacionales o por autorización excepcional.

Previo a comenzar la explotación o la prestación, deben comunicarlo al Registro de operadores, dependiente del Ministerio de Industria, Energía y Turismo, y someterse a las condiciones previstas para el ejercicio de la actividad que se quiera realizar.

La instalación, la explotación de redes públicas y la prestación de los servicios a terceros por operadores controlados directa o indirectamente por administraciones públicas, se debe realizar dando cumplimiento al principio de inversor privado, separando cuentas, atendiendo a la neutralidad, a la transparencia, a la no distorsión de la competencia y a la no discriminación.

Conforme se dispone en el artículo 9 de la LGT, una Administración Pública sólo podrá instalar y explotar redes o prestar servicios de comunicaciones electrónicas a terceros, a través de entidades o sociedades que tengan entre su objeto social o finalidad instalar y explotar redes o prestar servicios de comunicaciones. En dichos casos: (i) los operadores tienen derecho a acceder a condiciones neutrales, objetivas, transparentes, equitativas y no discriminatorias a la infraestructura y a los recursos asociados; (ii) asimismo, tienen derecho a usar de forma compartida las infraestructuras y sus recursos asociados, que fueran instalados por operadores controlados directa o indirectamente por administraciones públicas; y (iii) si las administraciones públicas reguladoras o titulares del dominio público tienen la propiedad, total o parcial, o ejercen el control, directo o indirecto, de operadores que explotan redes o prestan servicios de comunicaciones, deben mantener una separación estructural entre dichos operadores y los organismos encargados de la regulación y gestión de los derechos de utilización del dominio público correspondiente.

Entre las obligaciones que tienen quienes exploten redes o presten servicios de comunicaciones, se encuentra la de suministrar información a las Autoridades Nacionales de Reglamentación de Telecomunicaciones, quien deberá garantizar su confidencialidad, al tiempo que motivar la solicitud, siendo proporcional al fin perseguido, para el cumplimiento de alguna de los siguientes objetivos:

- Atender necesidades estadísticas y elaborar informes sectoriales.
- Comprobar el cumplimiento de las condiciones de prestación o de explotación de los servicios.
- Verificar que operadores controlados, directa o indirectamente, por administraciones públicas cumplen con los requisitos legales.
- Evaluar si procede o no las solicitudes para usar espectro radioeléctrico y numeración.
- Comprobar que se usen de forma efectiva y eficiente las frecuencias, los números y las obligaciones derivadas del uso de la numeración, direccionamiento y denominación o de ocupar el dominio público.
- Definir los mercados de referencia, establecer condiciones específicas a los operadores con poder significativo de mercado, conocer cómo la evolución de las redes o de los servicios puede repercutir en los servicios mayoristas. Asimismo, se podrá pedir que los mayoristas brinden datos contables sobre el mercado minorista asociado al mercado mayorista.
- Comprobar el cumplimiento de la regulación ex ante, de las resoluciones que correspondan, así como de las obligaciones de servicio público y de carácter público, al tiempo que determinar los prestadores del servicio universal.
- Garantizar el acceso equivalente para los usuarios con discapacidad, quienes deben poder elegir entre empresas y servicios.
- Poner a disposición de los ciudadanos información o aplicaciones para poder comparar precios, cobertura y calidad de los servicios.
- Facilitar la coubicación o el uso compartido de elementos de redes y de los recursos asociados.
- Analizar la integridad y la seguridad de las redes y de los servicios.

- Cumplir las obligaciones que establezca el ordenamiento jurídico.
- Planificar el uso de fondos públicos destinados al despliegue de infraestructura.

Los operadores tienen el derecho y la obligación de negociar la interconexión para prestar servicios de comunicaciones electrónicas, a fin de garantizar la interoperabilidad. No hay limitaciones para la negociación entre los operadores, sin perjuicio de que se pueden adoptar medidas en relación a las empresas que tengan poder significativo de mercado[172].

Aquellos prestadores que tengan un poder significativo en el mercado, podrán ser objeto de medidas específicas por parte de la CNMC, en materia de: (i) transparencia, en relación a la interconexión y al acceso, (ii) no discriminación, que garantice que aplique medidas equivalentes en circunstancias semejantes, (iii) separación de cuentas, en la forma y del modo que se especifique, (iv) acceso a elementos o a recursos específicos de las redes y a su utilización, (v) control de precios, con objeto de garantizar precios competitivos y evitar precios excesivos y márgenes no competitivos.[173]

Para la prestación de los servicios se proporcionará los números, direcciones y nombres que sean necesarios para la efectiva prestación[174]. El Gobierno aprobará planes nacionales de numeración, direccionamiento y denominación, y el el MIET se encargará de otorgar dichos derechos y de que los procedimientos sean abiertos, objetivos, no discriminatorios, proporcionados y transparentes. Todos los operadores, fabricantes y comerciantes deben realizar las medidas necesarias para adoptar las decisiones adoptadas por el MIET en esta materia.

Los planes nacionales establecerán los servicios para lo que se podrán utilizar los números, las direcciones y los nombres, así como las condiciones para su uso, las cuales deben ser proporcionadas y no discriminatorias. Serán públicos, salvo aquellos aspectos que pudieran afectar la seguridad nacional, y podrán establecer procedimiento de selección competitiva o comparativa, respetando los principios de publicidad, concurrencia y no discriminación.

[172] Artículo 12 de la LGT.
[173] Artículo 14 de la LGT.
[174] Artículo 19 de la LGT.

Vale destacar que los abonados tienen el derecho de conservar el número telefónico que se haya sido asignado, independientemente del operador que le preste los servicios.[175]

Se establecen obligaciones de servicios público, buscando garantizar la existencia de determinados servicios de comunicaciones disponibles al público, de adecuada calidad, en todo el territorio, a través de una competencia y una libertad real de elegir, atendiendo los supuestos en que los usuarios finales no se vean atendidos de manera satisfactoria por el mercado[176]. Cuando el MIET, previo informe de CNMC, determine que el servicio ya se está prestando en competencia, en condiciones de precio, cobertura y calidad de servicio similar a aquellas en que los operadores designados deben prestarlos, podrá determinar el cese de la obligación de servicio público[177].

Por otra parte, se prevé el servicio universal, como el conjunto definido de servicios cuya prestación se quiere asegurar a todos los usuarios finales, independientemente de su ubicación, con una calidad determinada y un precio asequible[178]. En caso de que la prestación de los servicios no sea garantizada por el libre mercado, el MIET designará a uno o más operadores para que garanticen la prestación de manera que quede cubierto todo el territorio nacional. La designación se hará por real decreto, atendiendo los principios de eficiencia, objetividad, transparencia y no discriminación, para lo cual se utilizará un mecanismo de licitación pública para dichos servicios, prestaciones y ofertas. Se garantizará que la prestación se haga de forma rentable[179]. Para estos efectos, se crea el fondo nacional del servicio universal, a fin de garantizar la financiación del servicio universal, recibiendo los operadores sujetos a la obligación de prestar el servicio universal de este fondo lo correspondiente al coste neto que le supone dicha obligación[180].

Interesa señalar que por necesidades de defensa nacional, seguridad pública, vial, de las personas o la protección civil, el Gobierno puede imponer otras obligaciones de servicio público distintas a las de servicio universal a los operadores, previo informe de la CNMC, así como de la administración territorial competentes, por razones de: (i)

[175] Artículo 21 de la LGT.
[176] Artículo 23 de la LGT.
[177] Artículo 23.4 de la LGT.
[178] Artículo 25 de la LGT.
[179] Artículo 26 de la LGT.
[180] Artículo 27 de la LGT.

cohesión territorial, (ii) extensión del uso de nuevos servicios y tecnologías a la sanidad, a la educación, a la acción social y a la cultura, (iii) facilitar la comunicaciones entre determinados colectivos, que se encuentren en circunstancias especiales y estén insuficientemente atendidas, y (iv) disponer de servicios que comporten la acreditación de fehaciencia del contenido del mensaje remitido[181].

Para la prestación de los servicios de comunicaciones electrónicas, el despliegue de redes es fundamental. En este sentido, se le reconoce a los operadores el derecho de ocupar propiedad privada, siempre que sea necesario para la instalación de redes y que no haya otra alternativa técnica o económicamente viable, ya sea a través de su expropiación forzosa o de la declaración de servidumbre forzosa de paso, lo cual será realizado por el MIET, respetando los procedimientos, los trámites y dando las garantías necesarias a los titulares afectados por la expropiación forzosa[182].

Asimismo, tienen derecho a ocupar el dominio público en tanto sea necesario para el despliegue de la red pública de comunicaciones. Los titulares del dominio público deben garantizar el acceso en condiciones neutrales, objetivas, transparentes, equitativas y no discriminatorias, sin poder establecer derecho preferente[183].

Vale destacar que la normativa de cualquier Administración Pública que pudiere afectar el despliegue de redes, debe reconocer el derecho de ocupación del dominio público o de la propiedad privada. Dichas normas deberán, por lo menos: (a) ser publicadas en un diario oficial, (b) prever un procedimiento rápido, sencillo, eficiente y no discriminatorio de resolución de solicitudes de ocupación, (c) garantizar la transparencia de los procedimientos y que las normas aplicables fomenten una competencia leal y efectiva, y (d) garantizar el respeto de los límites impuestos a la intervención administrativa en protección de los derechos de los operadores[184].

Finalmente, interesa destacar que se prevé que los operadores pueden celebrar voluntariamente acuerdos entre sí para determinar las condiciones de ubicación o de uso compartido de sus infraestructuras, con sujeción a la normativa de defensa de la competencia. Al tiempo que las administraciones públicas fomentarán ese tipo de acuerdos, especialmente para el despliegue de elementos de las redes rápidas y

[181] Artículo 28 de la LGT.
[182] Artículo 29 de la LGT.
[183] Artículo 30 de la LGT.
[184] Artículo 31 de la LGT.

ultrarrápidas de comunicaciones. Sin perjuicio, se prevé que ubicación compartida de infraestructura y de recursos compartidos también puede ser impuesto de manera obligatoria a los operadores que tengan derecho a ocupar propiedad pública o privada[185]. En esta línea, también se prevé que se pueden establecer limitaciones al dominio público radioeléctrico, en tanto tiene como finalidad su aprovechamiento óptimo, evitar su degradación y mantener un nivel adecuado de calidad[186]; así como la posibilidad de acceder a infraestructura susceptible de alojar redes públicas de comunicaciones, siempre que dicho acceso no comprometa la continuidad y la seguridad de la prestación de los servicios de carácter público que en dichas infraestructuras realice su titular[187].

Como surge del preámbulo de la LGT, a fin de facilitar el despliegue de redes y la prestación de los servicios de comunicaciones electrónicas, la LGT simplifica, eliminando licencias y autorizaciones por parte de la administración para determinadas categorías. En esta línea, ya en la Ley 12/2012 de 26 de diciembre, buscando la liberalización del comercio y de algunos servicios, algunas licencias necesarias para el despliegue se sustituyeron por una declaración responsable. Así se aplica, por ejemplo en los supuestos en que previamente el operador hubiera presentación un plan de despliegue, el cual hubiere sido aprobado expresa o tácitamente, en caso de que trascurrido dos meses desde su presentación, la administración no hubiere dictado resolución expresa.

La declaración responsable deberá expresamente señalar el cumplimiento de los requisitos que resulten exigibles de acuerdo a la normativa vigente.

Entre las diversas obligaciones de los prestadores se destacan las siguientes:

- Garantizar el secreto de las comunicaciones conforme a los artículos 18.3 y 55.2 de la Constitución española, debiendo adoptar las medidas técnicas necesarias[188].

- Interceptar las comunicaciones que se autoricen de acuerdo con el artículo 579 de la Ley de Enjuiciamiento Criminal, en la Ley Orgánica 2/2002,

[185] Artículo 32 de la LGT.
[186] Artículo 33 de la LGT.
[187] Artículo 37 de la LGT.
[188] Artículo 39.1 y 40 de la LGT.

reguladora del control judicial previo del Centro Nacional de Inteligencia y en otras normas con rango de ley orgánica[189].

- Proteger los datos de carácter personal, para lo cual deben adoptar las medidas técnicas y de gestión adecuadas para preservar la seguridad en la explotación de su red o en la prestación de sus servicios, garantizando que: (i) solo el personal autorizado tenga acceso a los datos personales para los fines autorizados por la ley, (ii) proteger los datos personas almacenados o transmitidos de la destrucción accidental o ilícita, la pérdida o alteración accidentales o el almacenamiento, tratamiento, acceso o revelación no autorizados o ilícitos, (iii) se aplique efectivamente una política de seguridad con respecto al tratamiento de datos personales. La Agencia Española de Protección de Datos Personales podrá examinar las medidas adoptadas por los operadores que exploten redes o que presten servicios de comunicaciones, y podrá formular recomendaciones sobre las mejores prácticas con respecto al nivel de seguridad que deberá conseguirse[190].

- Gestionar adecuadamente los riesgos de seguridad que puedan afectar a sus redes y servicios a fin de garantizar la seguridad y evitar o reducir al mínimo el impacto de los incidentes de seguridad en los usuarios y en las redes interconectadas[191].

- Garantizar la integridad de las comunicaciones, asegurando la continuidad en la prestación de los servicios[192].

- Notificar al MIET las violaciones de la seguridad o pérdida de la integridad que hayan tenido un impacto significativo en la explotación de las redes o en los servicios[193].

- Garantizar servicios telefónicos disponibles al público a través de las redes públicas de comunicaciones en caso de fallo catastrófico de la red o en casos de fuerza mayor, y adoptarán las medidas necesarias para garantizar el acceso sin interrupciones a los servicios de emergencia.

[189] Artículo 39 de la LGT.
[190] Artículo 41 de la LGT.
[191] Artículo 44 .1 de la LGT.
[192] Artículo 44.2 de la LGT.
[193] Artículo 44.3 de la LGT.

- Atender los derechos de los usuarios finales conforme lo establecido en el Capítulo V de la LGT y en la Ley General para la Defensa de los Consumidores y Usuarios aprobado por el real decreto Legislativo 1/2007, de 16 de diciembre. Vale destacar que de los mismos se desprenden obligaciones para los prestadores de servicios. Entre dichos derechos, se destacan:[194]

  - El derecho a celebrar contratos por parte de los usuarios finales con los operadores que exploten redes o presten servicios de comunicaciones disponibles al público.

  - El derecho a resolver el contrato en cualquier momento. Incluso de forma anticipada y sin penalización en caso de modificación de las condiciones contractuales impuestas por el operador.

  - El derecho al cambio de operador, con conservación de los números del plan nacional de numeración en el plazo máximo de un día laborable.

  - El derecho a la información, que debe ser veraz, eficaz, suficiente transparente, comparable y estar disponible al público.

  - Los supuestos, plazos y condiciones en que el usuario final puede ejercer el derecho de desconexión.

  - El derecho a la continuidad del servicio y a obtener compensación automática por su interrupción.

  - El derecho a obtener información completa, comparable, pertinente, fiable, actualizada y de fácil consulta sobre la calidad de los servicios.

  - El derecho a elegir el medio de pago para el abono ente los comúnmente utilizados.

  - El derecho a acceder a los servicios de emergencia de forma gratuita.

  - El derecho a la facturación detallada, clara y sin errores.

[194] Artículo 47 de la LGT.

- El derecho a detener el desvío automático de llamadas efectuado a su terminal por parte de un tercero.

- El derecho a impedir la presentación de la identificación de su línea en las llamadas que genere o la presentación de la identificación de su línea al usuario que le realice una llamada.

- El derecho a impedir la presentación de la identificación de la línea de origen en las llamadas entrantes y a rechazar las llamadas entrantes en que dicha línea no aparezca identificada.

- Disponer de un servicio de atención al cliente, gratuito, que facilite información, atienda y resuelva quejas y reclamos, garantizando una atención personal directa.

Por orden del MIET se podrán fijar requisitos mínimos de calidad de servicio que serán exigibles a los prestadores, para evitar la degradación del servicio y la obstaculización o ralentización del tráfico en las redes. Asimismo, se podrán establecer parámetros de calidad que habrán de cuantificarse, para garantizar a los usuarios información completa, comparable, fiable y de fácil consulta[195].

Se podrá prever por real decreto condiciones básicas para el acceso de las personas con discapacidad a las tecnologías, productos y servicios relacionados con las comunicaciones[196].

Los operadores deberán proporcionar antes de la celebración de un contrato entre usuarios finales y los operadores, al menos la información que establece el Texto Refundido de la Ley General para la Defensa de los Consumidores y Usuarios aprobado por el Real Decreto Legislativo 1/2007. Además, también antes de celebrar el contrato informarán al menos:

- Descripción de los servicios a proveer y posibles limitaciones en su uso.

- Los precios y tarifas aplicables.

- Duración del contrato y causas de resolución.

- Restricciones impuestas en cuanto a la utilización del terminal suministrado.

[195] Artículo 50 de la LGT.
[196] Artículo 52 de la LGT

- Condiciones aplicables en relación con la conservación de números.

Finalmente, interesa señalar que los operadores o quienes realicen las actividades a las que se refiere la LGT están obligados a facilitar al personal de inspección, en el ejercicio de sus funciones, el acceso a sus instalaciones. También deberán permitir que dicho personal lleve a cabo el control de los elementos afectados a los servicios o actividades que realicen, de las redes que instalen o exploten y de cuantos documentos están obligados a poseer o conservar. En este sentido, quedan obligados a poner a disposición del personal de inspección cuantos libros, registros y documentos, sea cual fuere su soporte, y medios técnicos éste considere precisos, incluidos los programas informáticos y los archivos magnéticos, ópticos o de cualquier otra clase. Asimismo, deberán facilitarles, a su petición, documentación que se les exija para la determinación de la titularidad de los equipos o la autoría de emisiones o actividades[197].

VI. Consideraciones finales

En Uruguay para poder prestar los servicios de telecomunicaciones, se requiere de actos administrativos, dictados por el Poder Ejecutivo, que expresamente lo autoricen. En España las autorizaciones no deben ser expresas y no son por tipos de servicios, y una de las principales casusas que se identifica para la Revolución TIC fue justamente la liberalización de las telecomunicaciones y los beneficios económicos que conlleva.

Nos encontramos ante actividad privada, de interés público, que se rige por el principio de libre y sana competencia, salvo las excepciones legalmente dispuestas.

Las autorizaciones y/o licencias son por clases de servicios en Uruguay, además los actos administrativos disponen el alcance, los requisitos y las condiciones, así como los derechos y las obligaciones que se derivan de las mismas. En España el régimen ya evolucionó, no diferenciando por clases de servicios, y aplicando realmente el principio de neutralidad tecnológica.

Considerando –entre otras cosas–: (i) la convergencia, (ii) el cambio que se ha generado en los modelos tradicionales con la transformación digital, (iii) el gran desarrollo de las tecnologías de avanzada, (iv) que ahora prácticamente todo va por Internet, (v) que la competencia es cada vez mayor y no solo entre empresas del mismo segmento, (vi) que al cliente le es indiferente el medio a través del cual se le presta el servicio final, (vii) que se necesitan más inversiones en redes de telecomunicaciones de

[197] Artículo 73 de la Lgt.

última generación, siendo fundamental la utilización eficaz y eficiente de los recursos; la tendencia es la licencia única de telecomunicaciones –que habilite a prestar todos los servicios de telecomunicaciones, fijos o móviles, alámbricos o inalámbricos, con o sin infraestructura propia–, y la compartición de infraestructura y de espectro radioeléctrico.

Para que la transformación digital se pueda desarrollar debidamente, el despliegue de redes de última generación es fundamental, siendo necesario, entre otras cosas: otorgar seguridad, reglas claras, dar previsibilidad, atender el principio de neutralidad tecnológica, la convergencia y la compartición de los recursos, así como hacer los ajustes y las actualizaciones regulatorios que sean necesarias.

CAPÍTULO IV: USO DEL ESPECTRO RADIOELÉCTRICO PARA LOS SERVICIOS DE TELECOMUNICACIONES[198]

I. Introducción

El espectro radioeléctrico (ER) es fundamental para el desarrollo de las comunicaciones inalámbricas y para el despliegue de las nuevas tecnologías.

Es un recurso natural, intangible, compartido, limitado, escaso, que se divide en bandas de frecuencias, a través de las cuales se transmiten las ondas electromagnéticas de los servicios de comunicación inalámbrica. Es muy requerido y su demanda está en alza, en tanto es necesario para el desarrollo de diversos servicios y aplicaciones, como ser: servicios de voz móviles, banda ancha móvil y fija, wi-fi, televisión para abonados, televisión digital terrestre, Internet de las Cosas, entre otros múltiples ejemplos.

Es parte del dominio público de los Estados, quienes lo administran, gestionan y controlan a nivel nacional; mas la UIT tiene un rol fundamental en la gestión, coordinación y compartición del ER a nivel mundial.

Es definido como *"la porción del espectro electromagnético (fenómeno por el cual se transmiten las ondas electromagnéticas) que se utiliza para las telecomunicaciones (radio, televisión, telefonía móvil, radares, satélites, etc.). El espectro radioeléctrico convencionalmente se fijó entre los 8,3 kHz y los 3,000 ghz y se dividió en bandas de frecuencia que son atribuidas a los diferentes servicios de telecomunicaciones*[199]*. Esta atribución considera para cada banda sus características específicas en términos de propagación de la señal, lo que las hace más adecuadas para la provisión de servicios específicos (ver tabla 1)*[200]*"*

---

198 Véase nuestro trabajo, ARAMENDIA, MERCEDES en "Estudios sobre los Desafíos Jurídicos ante la Digitalización", Universidad de Montevideo, 2019, pp. 183 y ss.

199 Reglamento de Radiocomunicaciones de la UIT,Volumen 1, Capítulo 1: terminología y características técnicas. Citado en "Directrices de política y aspectos Económicos de Asignación y Uso del Espectro Radioeléctrico". URL: https://www.itu.int/dms_pub/itu-d/opb/pref/D-pref-ef.rad_spec_guide-2016-pdf-S.pdf Consultado el 20 de febrero de 2019.

200 Unión Internacional de Telecomunicaciones: "Directrices de política y aspectos Económicos de Asignación y Uso del Espectro Radioeléctrico". URL: https://www.itu.int/dms_pub/itu-d/opb/pref/D-pref-ef.rad_spec_guide-2016-pdf-S.pdf Consultado el 20 de febrero de 2019.

Tabla 1: Usos y Propiedades de Bandas del Espectro Radioeléctrico

Banda	Rango de Frecuencia	Alcance	Utilización Común	Ancho de Banda	Interferencia
vlf (ondas milimétricas)	3-30 khz	1.000 km	Radionavegación de largo alcance	Muy estrecha	De amplia distribución
lf (ondas kilométricas)	30-300 khz	1.000 km	Radionavegación de largo alcance	Muy estrecha	De amplia distribución
mf (ondas hectométricas)	300-3.000 khz	2-3.000 km	Radionavegación de largo alcance	Moderada	De amplia distribución
hf (ondas decamétricas)	3-30 mhz	Hasta 1.000 km	Fijos punto a punto y Radiodifusión a nivel mundial	Amplia	De amplia distribución
vhf (ondas métricas)	30-300 mhz	2-300 km	Radiodifusión, Móviles, wan	Muy amplia	Confinada
uhf (ondas decimétricas)	300-3.000 mhz	< 100 km	Radiodifusión, Móviles, satelital	Muy amplia	Confinada
shf (ondas centimétricas)	3-30 ghz	30-2.000 km	Fijos, Radiodifusión, móviles, wan,	Muy amplia hasta 1 ghz	Confinada

			comunicaciones por satélite		
ehf (ondas milimétricas)	30 - 300 ghz	20 - 2000 km	Radiodifusión, fijos punto a punto, móviles, comunicaciones por satélite	Muy amplia hasta 10 ghz	Confinada

Fuente: ITU 2011 ICT Regulation Toolkit. Gestión del Espectro Radioeléctrico. Módulo 5, p. 14 (www.ictregulationtoolkit.org/en/home). Citado en Directrices de política y aspectos Económicos de Asignación y Uso del Espectro Radioeléctrico.[201]

En tanto recurso escaso, es esencial que sea administrado, gestionado y controlado adecuadamente, a fin de buscar su uso eficiente, al tiempo de promover el desarrollo, la optimización y la utilización de nuevos servicios radioeléctricos, redes y tecnologías.[202]

La política de espectro juega un papel muy importante en el ámbito económico y social por la importancia creciente que tienen las telecomunicaciones por sí mismas, así como por el impacto que tienen en otras industrias y servicios. Son fundamentales para la transformación digital, para la conectividad, para el acceso y para el desarrollo de los servicios inalámbricos, móviles y fijos; lo cual es esencial para disminuir la brecha digital, facilitar la innovación, promover la educación, universalizar nuevas tecnologías y desarrollar la economía digital.

II. La Unión Internacional de las Telecomunicaciones (uit) y el Espectro Radioeléctrico[203]

Como surge del punto 64 de la Declaración de Principios de Ginebra aprobada en la Cumbre Mundial sobre la Sociedad de la Información, el rol de la UIT,entre otras

201 Ibídem, pp. 2.
202 Considerando I del Decreto Nº 114/003 de Uruguay.

203 Véase nuestro trabajo, ARAMENDÍA, MERCEDES, "Aspectos fundamentales de los servicios de telecomunicaciones en el país" en *Estudios de Telecomunicaciones y Sociedad de la Información*, Universidad de Montevideo, 2018, págs. 55 y ss.

cosas, para la gestión del espectro radioeléctrico, reviste crucial importancia en la construcción de la Sociedad de la Información.[204]

Como ya se desarrolló anteriormente, la UIT es el organismo de las Naciones Unidas para las TIC[205], cuenta con 193 países miembros y más de 700 entidades del sector privado e instituciones académicas. Los miembros tienen los derechos y están sujetos a las obligaciones previstas en la Constitución y en el Convenio de la uit.

El Convenio y la Constitución de la UIT son los instrumentos fundamentales de la UIT,los cuales se complementan con Reglamentos Administrativos, como ser el Reglamento de las Telecomunicaciones Internacionales y el Reglamento de Radiocomunicaciones; regulan el uso de las telecomunicaciones y tienen carácter vinculante para todos los Miembros.

Como surge del Preámbulo de la Constitución de la UIT,se reconoce en toda su plenitud el derecho soberano de cada Estado a reglamentar sus telecomunicaciones; sin perjuicio, los Miembros están obligados a atenerse a las disposiciones de la Constitución, del Convenio y de los Reglamentos Administrativos en todas las oficinas y estaciones de telecomunicaciones instaladas o explotadas por ellos y que presten servicios internacionales o puedan causar interferencias perjudiciales a los servicios de radiocomunicación de otros países, excepto en lo relativo a las instalaciones radioeléctricas militares conforme el artículo 37 de la Constitución de la UIT. Además, los Miembros deben adoptar las medidas necesarias para imponer observancia de las disposiciones de los instrumentos de la Unión a las empresas de explotación por ellos autorizadas, para establecer y explotar telecomunicaciones y que presten servicios internacionales o que exploten estaciones que puedan causar interferencias perjudiciales a los servicios de radiocomunicación de otros países.

La UIT,entre otras cosas: (i) efectúa la atribución y adjudicación de las bandas de frecuencias del espectro radioeléctrico, y lleva el registro de las asignaciones de frecuencias y las posiciones orbitales asociadas en la órbita de los satélites geoestacionarios, a fin de evitar toda interferencia perjudicial entre las estaciones de

204 Declaración de Principios de Ginebra de la Cumbre Mundial sobre la Sociedad de la Información. URL: https://www.itu.int/net/wsis/docs/geneva/official/dop-es.html Consultado el 5 de febrero de 2019.

205 Sobre la UIT: https://www.itu.int/es/about/Pages/default.aspx Consultado el 5 de febrero de 2018.

radiocomunicaciones de los distintos países; (ii) coordina esfuerzos para eliminar interferencias perjudiciales entre las estaciones de radiocomunicaciones de los diferentes países y para mejorar la utilización del espectro de frecuencias radioeléctricas y de la órbita de los satélites geoestacionarios para los servicios de radiocomunicación; (iii) facilita la normalización mundial de las telecomunicaciones con una calidad de servicio satisfactoria.

La Constitución de la UIT establece disposiciones generales relativas a las telecomunicaciones y en relación al ER,señala entre otras cosas que: (i) se debe procurar limitar las frecuencias y el espectro utilizado para obtener el funcionamiento satisfactorio de los servicios, para ello los Miembros se deben esforzar por aplicar, a la mayor brevedad, los últimos adelantos de la técnica; (ii) en la utilización de bandas de frecuencias para las radiocomunicaciones, los Miembros deben tener en cuenta que las frecuencias y la órbita de los satélites geoestacionarios, son recursos naturales limitados que deben utilizarse de forma racional, eficaz y económica, de conformidad con lo establecido en el Reglamento de Radiocomunicaciones; y (iii) todas las estaciones deben ser instaladas y explotadas de manera de no causar interferencias perjudiciales a las comunicaciones o servicios radioeléctricos de otros Miembros.

La UIT cumple un rol esencial en lo que respecta a la evolución de las tecnologías y a la gestión global del uso del ER,a través de la aprobación de reglamentos internacionales, normas, recomendaciones, informes, etc.; siendo la coordinación un elemento fundamental para el uso eficiente del ER y para evitar interferencias perjudiciales.

Considerando el contexto actual, hay una demanda constante y creciente de ER,lo cual genera nuevos desafíos, destacándose entre los principales problemas: la escasez de los recursos radioeléctricos y el aumento del coste de acceso al ER,reconociendo que ya no se trata de un tema técnico y administrativo, sino que intervienen también aspectos económicos, financieros y sociales.[206]

La UIT reconoce que la escasez de frecuencias y el aumento de los costos de acceso al ER se debe principalmente por los siguientes factores: *(i) la desreglamentación y liberalización de los mercados de comunicaciones electrónicas;*

206 Unión Internacional de Telecomunicaciones, Resolución Nº 9 del 2014. URL: https://www.itu.int/dms_pub/itu-d/opb/stg/D-stg-sg02.res09.1-2014-pdf-S.pdf Consultado el 20 de febrero de 2019.

(ii) la privatización y comercialización del dominio público; (iii) la toma de conciencia del valor del espectro; y (iv) la competencia mundial entre operadores multinacionales[207].

Como consecuencia, la UIT entiende que la gestión del espectro debe abarcar tres áreas: (i) planificación: presente y futura, (ii) administración: autorizaciones, licencias, compatibilidad de los usos y equipos, y (iii) monitoreo y control. Lo cual requiere procesos regulatorios, como son: la atribución, la adjudicación y la asignación.[208]

Al respecto, el artículo 1 del Reglamento de Radiocomunicaciones de la UIT,en la Sección II, define:

i. a la *"atribución de una banda de frecuencia"* como la "*Inscripción en el Cuadro de atribución de bandas de frecuencias, de una banda de frecuencias determinada, para que sea utilizada por uno o varios servicios de radiocomunicación terrenal o espacial o por el servicio de radioastronomía en condiciones especificadas. Este término se aplica también a la banda de frecuencias considerada"*;

ii. a la "*adjudicación de una frecuencia o de un canal radioeléctrico*" como la *"Inscripción de un canal determinado en un plan, adoptado por una conferencia competente, para ser utilizado por una o varias administraciones para un servicio de radiocomunicación terrenal o espacial en uno o varios países o zonas geográficas determinados y según condiciones especificadas"*

iii. a la "*asignación de una frecuencia o de un canal radioeléctrico*" como la *"Autorización que da una administración para que una estación radioeléctrica utilice una frecuencia o un canal radioeléctrico determinado en condiciones especificadas."*

La UIT señala en la Resolución Nº 9/2014 que: *"tradicionalmente, los poderes públicos solían atribuir las frecuencias para aplicaciones determinadas, y luego asignaban partes del espectro a entidades encargadas de utilizarlo con fines concretos, aplicando el principio de "primero en llegar, primero en ser servido". Este método resultaba rápido, práctico y menos oneroso, pero tiene sus limitaciones en el contexto de la competencia vigente hoy en día"*.

---

207 Ibídem.

208 UIT, "Directrices de política y aspectos económicos de asignación y uso del espectro radioeléctrico", URL: https://www.itu.int/dms_pub/itu-d/opb/pref/D-PREF-EF.RAD_SPEC_GUIDE-2016-PDF-S.pdf Consultado el 20 de febrero de 2019.

Se reconoce la necesidad de una gestión moderna que optimice el valor del ER,para lo cual se debe considerar: (i) la eficiencia económica: la cual permite maximizar el valor agregado del uso de los servicios, todas las frecuencias pueden ser usadas para más de un servicio; (ii) la eficiencia técnica: implica definir las condiciones de uso y las tecnologías específicas, en tanto permiten reducir las interferencias, entendiendo por tales una degradación que se produce en la calidad de la comunicación por trasmisiones residuales de frecuencias vecinas; y (iii) el beneficio social: en tanto permite que los usuarios se beneficien con más cobertura y más competencia.[209]

En este sentido, considerando la demanda creciente para acceder a más espectro, se han definido diversos métodos a través de los cuales se puede asignar espectro[210].

A modo de ejemplo:

1. Sorteo: el cual se realiza entre entidades similares o equivalentes.

2. Método de evaluación comparativo: permite elegir entre diversas solicitudes equivalentes, pueden basarse en varios criterios de calificación y de selección, los cuales son publicados previamente y los candidatos intentan demostrar que se ajustan de mejor forma a los criterios definidos.

3. Subasta: se termina definiendo por el mercado, se determinan previamente los criterios –técnicos, financieros y comerciales– y generalmente se limita la participación.

Hay distintos tipos, entre los más comunes se destacan: (i) Subasta abierta (oferta pública) o cerrada (en sobre cerrado); (ii) Subasta simple (una vuelta) o de múltiples vueltas; (iii) Subasta de un solo objeto o varios; (iv) Subasta abierta secuencial o simultánea; (v) Subasta inglesa (al alza); (vi) Subasta holandesa (a la baja).

Además, puede haber combinaciones, por ejemplo: subasta al alza simultánea a múltiples vueltas.

4. Mercado del espectro secundario: es la compra y la venta de licencias o de autorizaciones de uso de ER previamente atribuido.[211]

209 Ibídem.
210 UIT, Resolución Número 9 del 2014.
211 UIT, Resolución 9 del 2014.

III. Código Europeo de Comunicaciones Electrónica (CECE).

La Comisión Europea en su comunicado de 6 de mayo de 2015, por la que estableció la Estrategia para el Mercado Único Digital, dispuso entre otras necesidades, la importancia de revisar el marco de las telecomunicaciones, incentivando la inversión en redes de banda ancha de alta velocidad, buscando además un enfoque armonizado sobre la política y la gestión del espectro radioeléctrico.

El ER es un recurso público, escaso, con un importante valor público y de mercado, con valor social, cultural y económico, siendo un elemento esencial para el desarrollo de las redes y de los servicios de comunicaciones electrónicas basados en las radiocomunicaciones, por lo que debe ser asignado de forma eficiente por las autoridades correspondientes, en base a criterios objetivos, transparentes y no discriminatorios, teniendo en cuenta los intereses democráticos, sociales, lingüísticos y culturales, así como la Decisión Nº 676/2002/CE que establece un marco de armonización del espectro radioeléctrico.[212]

En esta línea, se prevé que la atribución de derechos individuales, la concesión de autorizaciones generales y la concesión de esos derechos por las autoridades competentes deben basarse en criterios objetivos, transparentes, favorables para la competencia, no discriminatorios y proporcionados[213].

Considerando la importancia del ER para el desarrollo del MUD, es fundamental que la regulación cubra el uso del ER para todas las redes de comunicaciones y que no se centre en una actividad específica. La tecnología evoluciona constantemente y ya en algunos países se está desplegando el 5G.

El 5G es la última generación de telefonía móvil, tiene muchos beneficios respecto a la tecnología 4G, sobre todo en lo que respecta a: (i) la velocidad, en 4G tenemos una velocidad promedio de 150 Mb/s y en 5G 20 Gb/s, (ii) la capacidad de almacenamiento, se va a necesitar menos memoria porque vamos a utilizar más en la nube, (iii) la calidad, (iv) la latencia, lo cual beneficia a dispositivos conectados y facilita el desarrollo de Internet de las cosas, sobre todo para la automoción y la salud, (v) la innovación, permitiéndonos disponer de más productos y servicios.

[212] Considerando (107) del Código Europeo de Comunicaciones Electrónicas.
[213] Artículo 45 del Código Europeo de Comunicaciones Electrónicas.

En este sentido, con la nueva tecnología de avanzada[214] el ER se comenzará a utilizar para otros fines como ser el transporte, la investigación, la sanidad en línea, la seguridad pública, atender catástrofes, Internet de las Cosas, la comunicación entre máquinas, los vehículos autónomos, entre otros múltiples ejemplos.

Todo lo anterior requerirá grandes inversiones, más consumo de datos, que dispongamos de equipos capaces de operar con la nueva tecnología, que despleguemos infraestructuras, siendo fundamental el uso eficaz y eficiente del ER, buscando evitar interferencias[215].

A medida que se desarrollan nuevos usos y aplicaciones, se requieren más capacidad de red, lo cual se refleja directamente en la necesidad de más ER, pero siendo cada vez más importantes aspectos como la latencia, la disponibilidad y la fiabilidad.

Se requieren redes de muy alta capacidad, con parámetros similares a los ofrecidos por la fibra óptica, y que puedan ser utilizadas de forma generalizada, por todos, a un precio razonable, promoviendo la innovación, el uso eficiente de los recursos, normas comunes, previsibilidad regulatoria y neutralidad tecnológica.

Teniendo en cuenta que el ER no conoce fronteras, para su utilización adecuada es fundamental planificar, coordinar y armonizar el uso, a fin de evitar interferencias. A estos efectos, se ve como necesario adoptar planes, como el dispuesto por la Decisión Nº 243/2012/UE del Parlamento Europeo y del Consejo, a fin de establecer orientaciones, objetivos de planificación, así como la armonización en la utilización del ER en la UE.

La fragmentación de políticas afecta la innovación y el desarrollo, por lo que es importante:

Buscar coherencia entre lo que estable la UE y otras organizaciones internacionales que atienden la materia como es la UIT y la Conferencia Europea de Administraciones Postales y de Telecomunicaciones (CEPT).

Alcanzar una adecuada coordinación, a fin de evitar interferencias perjudiciales, a través del Grupo de Políticas del Espectro Radioeléctrico (RSPG), creado por la Decisión 2002/622/CE de la Comisión para el desarrollo del mercado interior y de la

[214] Como puede ser: blockchain, inteligencia artificial, internet de las cosas, almacenamiento en la nube, big data e impresoras 3D, entre otros ejemplos.
[215] Considerando (12) del Código Europeo de Comunicaciones Electrónicas.

política del ER,en base a consideraciones económicas, políticas, culturales, estratégicas, sanitarias y sociales.

Flexibilizar el uso, establecer autorizaciones neutras, tanto en relación a la tecnología, como respecto de los servicios, para poder elegir las mejores. Las determinaciones previas de las tecnologías y de los servicios solo deben admitirse cuando haya razones de interés general que así lo requieran, se debe atender el principio de neutralidad tecnológica y el principio de neutralidad del servicio.

El uso compartido del ER para poder hacer un uso más eficaz y eficiente, facilitando el acceso y el despliegue de redes. La demanda aumenta constantemente en tanto se requiere para las nuevas tecnologías y aplicaciones que se desarrollan.

Distintos tipos de autorizaciones: en algunos casos las autorizaciones generales pueden ser más eficaces en tanto fomentan la innovación y la competencia; sin embargo, en otros supuestos, las autorizaciones individuales pueden ser más apropiadas, como por ejemplo cuando por las características de propagación del ER las autorizaciones generales no podrían afrontar la interferencia.

Atender la duración de las autorizaciones y la posibilidad de renovar el derecho de uso para alcanzar una gestión continua de los recursos.

En definitiva, en la gestión del ER, los Estados fomentarán[216]: (i) armonizar el uso; (ii) un uso efectivo y eficiente; (iii) la competencia, economías de escala y la interoperabilidad de los servicios y de las redes; (iv) cubrir el territorio y la población con alta calidad y velocidad; (v) desarrollar nuevas tecnologías y aplicaciones inalámbricas; (vi) la inversión a largo plazo, para lo cual darán previsibilidad y coherencia en las concesiones, renovaciones, modificaciones, restricciones o supresiones de los derechos para utilizar el ER; (vii) prevenir interferencias perjudiciales transfronterizas o nacionales; (viii) el uso compartido del ER; (ix) flexibilidad en el sistema de autorización; (x) normas claras, que den certidumbre, coherencia y previsibilidad; (xi) revisión periódica; (xii) uso de todo tipo de tecnología; (xiii) se podrán prever restricciones para evitar interferencias perjudiciales, proteger la salud pública frente a los campos electromagnéticos, asegurar la calidad técnica del servicio, garantizar el uso compartido, eficiente y el logro de los objetivos de interés general; y (xiv) que se pueda brindar todo tipo de servicios de comunicaciones

[216] Artículo 45 del Código Europeo de Comunicaciones Electrónicas.

electrónicas y si se deben establecer restricciones, que sean para la seguridad de la vida, la coherencia social, evitar el uso ineficiente, promover la diversidad cultural y lingüística, así como el pluralismo de los medios de comunicación, debiendo revisarse periódicamente.

En relación a la autorización para el uso del ER, se destaca que los Estados miembros deben facilitar la utilización compartida del ER, en el marco de autorizaciones generales, limitando las concesiones individuales para aquellas situaciones en que sea necesario para maximizar el uso eficiente. A estos efectos, se deberá tener en cuenta: (i) las características del ER,(ii) la protección contra interferencias perjudiciales, (iii) la compartición fiable del ER,(iv) la calidad de las comunicaciones o del servicio, (v) el interés general y (vi) garantizar el uso eficiente[217].

Las Administraciones deben garantizar un uso eficaz y eficiente del ER, para lo cual pueden disponer: (i) compartir infraestructuras pasivas o activas o el ER; (ii) celebrar acuerdos comerciales para el acceso; y (iii) desplegar conjuntamente infraestructuras para el suministro de redes o servicios[218].

Si fuere necesario otorgar derechos individuales de uso del ER, se otorgarán a cualquier empresa para la prestación de redes o servicios, previa solicitud, garantizando un uso eficiente. Sin embargo, para la asignación de ER para los proveedores de servicios de contenidos radiofónicos o televisivos de interés general, los derechos individuales se otorgarán mediante procedimientos abiertos, objetivos, transparentes, no discriminatorios y proporcionales. No se requerirá que sea un procedimiento abierto cuando sea necesario para lograr objetivos de interés general, definidos por los Estados miembros. Los criterios de elegibilidad serán fijados de antemano y serán: objetivos, transparentes, proporcionados, no discriminatorios y reflejarán las condiciones asociadas. Los titulares de derechos individuales podrán cederlos o arrendarlos conforme a lo que establezcan los Estados miembros y en las condiciones que dispongan[219].

Los derechos individuales de uso serán por un plazo limitado, adecuado para la amortización de las inversiones, buscando garantizar la competencia, el uso eficaz y

[217] Artículo 46 del Código Europeo de Comunicaciones Electrónicas.
[218] Artículo 47 del Código Europeo de Comunicaciones Electrónicas.
[219] Artículo 48 del Código Europeo de Comunicaciones Electrónicas.

eficiente, promover la innovación y la inversión[220]. En esta línea, se dará a los titulares de los derechos, un período mínimo de veinte años de previsibilidad normativa, que respeten las condiciones de inversión, y se prevé la prórroga de la duración de los derechos de uso, en vista de la necesidad de: (a) garantizar el uso eficaz y eficiente del ER,(b) atender los objetivos de interés general, como son: proteger la seguridad de la vida humana, el orden público, la seguridad pública o la defensa, y (c) asegurar una competencia real[221].

En relación a este último punto se prevé el derecho al acceso por parte de las empresas y la obligación de dar interconexión, con el fin de prestar servicios de comunicaciones electrónicas; así como el análisis del mercado y la determinación de empresas con peso significativo en el mercado.

Se considera que una empresa tiene "peso significativo en el mercado¨ cuando individual o conjuntamente con otras, tiene una posición de fuerza que le habilita a actuar de forma independiente a los competidores y clientes. Se prevén procedimientos para identificar y definir el mercado, obligaciones específicas para las empresas con peso significativo en el mercado, como ser: transparencia, no discriminación, mantener cuentas separadas, acceso y uso de elementos de las redes y recursos asociados, entre otros ejemplos.

Se prevé que a más tardar el 21 de diciembre de 2020, el ORECE publicará directrices sobre los criterios para que una red sea considerada de muy alta capacidad, determinando el ancho de banda disponible, la resiliencia, los parámetros de error, la latencia y la variación[222].

IV. El espectro radioeléctrico en la regulación de España

Se parte de la base de que el ER es un recurso fundamental para la prestación de muchos servicios y que tiene gran importancia para nuestra vida y para nuestra economía.

La Agenda Digital de España comentada anteriormente, incorpora los objetivos de la Agenda Digital para Europa, entre los cuales se destaca que para el año 2020 todos

[220] Artículo 49 del Código Europeo de Comunicaciones Electrónicas.
[221] Artículo 49 del Código Europeo de Comunicaciones Electrónicas.
[222] Artículo 82 del Código Europeo de Comunicaciones Electrónicas.

los ciudadanos tengan acceso a banda ancha de calidad, con velocidades mínimos de 30 Mbps.

La LGT Nº 9/2014, es la base normativa de la materia, facilitando el despliegue de infraestructura para la prestación de los servicios, así como poner a disposición de los ciudadanos servicios de calidad.

Para que esto último sea posible, el ER es fundamental en tanto es el soporte para las telecomunicaciones móviles, siendo un recurso estratégico, muy valioso y requerido, siendo esencial una regulación adecuada para flexibilizar el acceso, así como su uso eficaz y eficiente.

El artículo 60 de la LGT dispone que el ER es un bien de dominio público y que su titularidad y administración corresponden al Estado. La administración debe realizarse considerando su valor social, cultural y económico, así como la necesidad de cooperación en la planificación, coordinación y armonización del uso con otros estados miembros de la Unión Europea y con la Comisión Europea. Teniendo como principios: (i) garantizar un uso eficaz y eficiente, (ii) fomentar la neutralidad tecnológica y de los servicios, así como el mercado secundario de espectro, y (iii) fomentar una mayor competencia.

Para asegurar la armonización se debe: (i) planificar la utilización; (ii) gestionar, en base a los planificado, las condiciones técnicas y el otorgamiento de los derechos; (iii) controlar las emisiones, las interferencias, inspeccionar equipos, instalaciones y aparatos electrónicos; (iv) aplicar el régimen sancionador.

Se prevé que el Gobierno desarrolle por real decreto las condiciones para la adecuada administración del dominio público radioeléctrico, previendo: (a) el procedimiento para elaborar los planes de utilización del ER; (b) el procedimiento de determinación, control e inspección de los niveles de emisión radioeléctrica tolerables, que no supongan un riesgo para la salud humana; (c) los procedimientos, plazos y condiciones para la habilitación de los derechos de uso del dominio público radioeléctrico, que serán autorizaciones generales o individuales, afectación o concesión administrativa; (d) el procedimiento para la reasignación del uso de bandas de frecuencias; (e) las condiciones no discriminatorias, proporcionadas y transparentes asociadas a los títulos habilitantes para el uso del dominio público radioeléctrico; (f) las

condiciones para otorgar títulos habilitantes para el uso del dominio público; y (g) la adecuada utilización del ER mediante el empleo de equipos y aparatos.

Conforme lo dispuesto en el artículo 62 de la LGT, los títulos habilitantes para el uso del ER podrán ser: común, especial o privativo. El uso común no requiere título habilitante y se lleva a cabo en las bandas de frecuencias y con las características técnicas que se establezcan. El uso especial es el que se realiza de las bandas de frecuencias habilitadas para su explotación de forma compartida, sin límite al número de operadores o usuarios, con las condiciones técnicas y para los servicios que se establezcan. El uso privativo es el que se realiza mediante la explotación exclusiva o por un número limitado de usuarios de determinadas frecuencias, en un mismo ámbito físico de aplicación.

Los títulos habilitantes a través de los cuales se otorgan los derechos de uso, pueden ser: autorizaciones generales, autorizaciones individuales, afectación o concesión administrativa.

Las autorizaciones generales aplicarán en los casos de uso especial de las bandas de frecuencias habilitadas a dichos efectos, instaladas o explotadas por operadores de comunicaciones electrónicas. Se entienden concedidas sin más trámite que la notificación a la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información, conforme los requisitos establecidos por el Ministerio de Industria, Energía y Turismo.

Las autorización individual se utilizarán cuando: (i) se trate de una reserva de derecho de uso especial por radioaficionados u otros sin contenido económico en cuya regulación específica así se establezca; y (ii) se otorgue el derecho de uso privativo para auto prestación por el solicitante, salvo para las administraciones públicas, que requerirán de afectación demanial. Sin perjuicio de estos casos, en los demás supuestos se requiere una concesión administrativa, para lo cual es requisito previo que el solicitante sea operador de comunicaciones electrónicas y que no concurra alguna prohibición de contratar conforme lo dispuesto en el real decreto Legislativo 3/2011, Ley de Contratos Públicos.

Será competente para el otorgamiento de los títulos habilitantes la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información, salvo en los casos en que el título habilitante se otorgue por procedimiento de licitación.

En este último supuesto, conforma lo dispuesto en el artículo 63 de la LGT, cuando sea necesario garantizar el uso eficaz y eficiente del espectro radioeléctrico, en vistas de alcanzar los máximos beneficios para los usuarios y promover la competencia, el Ministerio de Industria, Energía y Turismo podrá, previa audiencia a las partes interesadas, limitar el número de concesiones demaniales a otorgar sobre dicho dominio para la explotación de redes públicas y la prestación de servicios de comunicaciones electrónicas. En todo caso se respetarán los principios de publicidad, concurrencia y no discriminación para todas las partes interesadas.

Los títulos habilitantes son otorgados por un plazo determinado.

Los derechos de uso privativo sin limitación de número: se otorgarán por períodos de cinco años, finalizando el 31 de diciembre del año en el que se cumpla el quinto año. Pueden ser renovables, por períodos de cinco años, dependiendo de la disponibilidad y de la planificación. Se podrá fijar un período de duración distinto.

Los derechos de uso privativo con limitación de número: dependerá de cada procedimientos de licitación, pero será como máximo de veinte años, incluyendo posibles prórrogas y sin posibilidad de renovación automática. Para su determinación, se tendrá en cuenta, entre otras cosas: las inversiones, los plazos de amortización y las obligaciones vinculadas (por ejemplo: cobertura mínima que se imponga, y las bandas de frecuencias cuyos derechos de uso se otorguen).

El Ministerio de Industria, Energía y Turismo podrá modificar los títulos habilitantes para el uso del dominio público radioeléctrico, previa audiencia del interesado, en vista de los principios de objetividad y de proporcionalidad, atendiendo las necesidades de planificación, el uso eficiente y la disponibilidad del ER.

Se prevé específicamente la neutralidad tecnológica y de servicios para el uso del ER, previendo que se podrá utilizar cualquier tipo de tecnología para los servicios de comunicaciones electrónicas, siempre que sea de conformidad con el Derecho de la Unión Europea.

Sin perjuicio, se podrán prever restricciones a los tipos de tecnología, en tanto sean proporcionadas y no discriminatorias, cuando sea necesario para: (a) evitar interferencias perjudiciales, (b) proteger la salud pública frente a los campos electromagnéticos, (c) asegurar la calidad técnica del servicio, (d) garantizar un uso

compartido[223] y eficiente del ER, y (f) alcanzar el logro de un objetivo de interés general[224].

Asimismo, se podrán prever restricciones a los tipos de servicios a prestar en determinada banda, cuando sea necesario para lograr objetivos de interés general establecidos de acuerdo con el Derecho de la Unión Europea, como por ejemplo: (a) asegurar la vida, (b) promover la cohesión social, regional o territorial, (c) evitar el uso ineficiente de las radiofrecuencias, y (d) promover la diversidad cultural, lingüística y el pluralismo de los medios de comunicación[225].

No obstante, se prevé que la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información debe revisar periódicamente la pertinencia de las restricciones.

Interesa destacar que los títulos habilitantes para el uso del ER pueden ser transferidos y los derechos de uso cedidos, ya sea de forma total o parcial, en las condiciones que se establezcan mediante real decreto. En ningún caso la cesión eximirá al titular de las obligaciones asumidas frente a la Administración.

En el año 2017 se aprobó el Real Decreto Nº 123/2017, con el objeto de desarrollar la Ley General de Telecomunicaciones Nº 9/2014 en relación al uso del dominio público radioeléctrico.

Define al "dominio público radioeléctrico" como *"el espacio por el que que pueden propagarse las ondas radioeléctricas. Se entiende por espectro radioeléctrico las ondas electromagnéticas cuya frecuencia se fija convencionalmente por debajo de 3000 gigahertzios que se propagan por el espacio sin guía artificial.*[226]*"*

[223] El artículo 13 del Real Decreto Nº 123/2017 dispone que: "el uso compartido del dominio público radioeléctrico permite el uso de una banda o de un rango de frecuencias por parte de varios usuarios, a los que se otorgan derechos de uso de dichas frecuencias en un mismo ámbito geográfico". A dichos efectos, prevé que los titulares de los derechos de uso compartido con otros titulares, deben aceptar las limitaciones y restricciones, e incorporar a sus redes los dispositivos técnicos que sean pertinentes. Además, a fin de alcanzar un uso más eficiente, señala la posibilidad de imponer el uso compartido por terceros, en caso de que haya en determinadas zonas geográficas infrautilización de los derechos de uso otorgados, y en caso de que la tecnología permita otorgar derechos de uso compartidos, sin menoscabar los derechos de uso inicialmente atribuidos.

[224] Artículo 66.1 del Código Europeo de Comunicaciones Electrónicas.

[225] Artículo 66.2 del Código Europeo de Comunicaciones Electrónicas.

[226] Artículo 3 del Real Decreto Nº 123/2017.

Se entiende que es un factor fundamental para el crecimiento económico, de interés público, social y cultural, siendo un recurso cada vez más estratégico, valioso y demandado, requiriendo un aprovechamiento efectivo y eficiente[227].

Los principios bases del Reglamento de ER son: (i) garantizar el uso eficaz, eficiente y flexible del ER; (ii) fomentar la competencia en el mercado de comunicaciones y facilitar la entrada de nuevos actores; (iii) promover la inversión eficiente, la certidumbre regulatoria y el despliegue de infraestructuras y de redes; (iv) favorecer el desarrollo de nuevos servicios, redes y tecnologías innovadoras; (v) contribuir al uso armonizado del ER; y (vi) garantizar la disponibilidad de ER para servicios públicos[228].

La administración del ER le compete al Estado, debiendo: (a) planificar la utilización del ER,(b) gestionar las condiciones técnicas de explotación y los derechos de uso, (c) controlar las emisiones radioeléctricas, el uso, los parámetros, las interferencias, así como su protección activa, y (d) aplicar el régimen sancionador[229].

La utilización el ER se efectúa de acuerdo con una planificación previa, realizada por la Secretaría de Estado para la Sociedad de la Información y la Agenda Digital.

En este sentido, se realizó el Cuadro Nacional de Atribución de Frecuencias (CNAF) para lograr la utilización coordinada y eficaz del ER,el cual debe ser aprobado por el Ministerio de Energía, Turismo y Agenda Digital para los distintos tipos de servicios de radiocomunicación. A través de CNAF se busca: reservar ER para determinados servicios, establecer preferencias para fines sociales, delimitar bandas para las Administraciones Públicas para la gestión de sus servicios, disponer las bandas que se utilizarán para fines privados, fomentar la neutralidad de red y de servicios, prever límites a la cantidad de espectro que podrá ser reservado para un mismo titular para promover la competencia[230].

Asimismo, se previó que le correspondía a la Secretaria de Estado para la Sociedad de la Información y la Agenda Digital elaborar los proyectos de planes

[227] Conforme a lo establecido en el artículo 12 del Real Decreto Nº 123/3017, se considera que el ER se utiliza eficazmente cuando el uso es efectivo y continuado en la zona geográfico para la cual fue reservado; y se entiende que el uso es eficiente cuando se garantizan los mismos objetivos de cobertura, capacidad y de transmisión y calidad del servicio, utilizando un menor consumo de los recursos espectrales.
[228] Artículo 2 del Real Decreto Nº 123/2017.
[229] Artículo 4 del Real Decreto Nº 123/2017.
[230] Artículo 6 del Real Decreto Nº 123/2017.

técnicos nacionales de radiodifusión sonora y de televisión, debiendo ser aprobados por el Gobierno, con el objetivo de alcanzar un uso racional, óptimo y eficaz del ER.

Por otra parte, se creó el Registro Nacional de Frecuencias[231] y el Registro Público de Concesiones[232], gestionados ambos por la Secretaría de Estado para la Sociedad de la Información y la Agenda Digital. El primero, para registrar los derechos de uso de frecuencias, disponiendo los titulares y las características de la explotación. El segundo, será un registro público, accesible a través de la sede electrónica del Ministerio Energía, Turismo y Agenda Digital, en el que constarán los datos públicos del Registro Nacional de Frecuencias relativos a los titulares de concesiones administrativas para el uso del ER.

Interesa señalar además lo dispuesto por el Real Decreto Nº 458/2011, sobre actuaciones en materia de ER para el desarrollo de la sociedad digital, persiguió, entre otras cosas, la introducción del principio de neutralidad tecnológica, la generalización de la neutralidad de servicios y la ampliación de las bandas de frecuencias en las que se puede efectuar la transferencia de títulos habilitantes o cesión de derechos de uso del dominio público radioeléctrico.

Se entiende por "neutralidad tecnológica" la posibilidad de utilizar los diferentes sistemas o tecnologías en distintas bandas de frecuencias, y por "neutralidad de servicios", la posibilidad de prestar servicios de comunicaciones electrónicas: fijos, móviles o nómadas[233].

En este sentido, en el artículo 2 del Real Decreto Nº 258/2011, se prevé como objetivos y principios relacionados con el ER los siguientes: (a) impulsar el desarrollo de la sociedad digital; (b) promover el uso como factor de desarrollo técnico, económico, de seguridad, del interés público, social y cultural; (c) garantizar un uso más eficaz y eficiente; (d) promover el desarrollo de nuevos servicios, redes y tecnologías; (e) fomentar una mayor competencia en el mercado de las comunicaciones electrónicas; (f) promover la realización de inversiones en infraestructuras; (g) impulsar la mayor extensión de la cobertura de los servicios de comunicaciones electrónicas; (h) fomentar la innovación; (i) generalizar la aplicación de los principios de neutralidad tecnológica y de servicios; y (j) ampliar las bandas de frecuencia en las que se puede efectuar la

[231] Artículo 8 del Real Decreto Nº 123/2017.
[232] Artículo 9 del Real Decreto Nº 123/2017.
[233] Artículo 3 del Real Decreto Nº 258/2011.

transferencia de títulos habilitantes o cesión de derechos de uso del dominio público radioeléctrico.

Se establecen límites a la disponibilidad de frecuencias por parte de un mismo operador a fin de promover la competencia y contribuir a neutralizar los posibles efectos derivados de la introducción del principio de neutralidad tecnológica.

Asimismo, se disponen condiciones específicas para las diversas bandas de frecuencias, en el siguiente orden: (i) 900 Mhz, (ii) 1800 Mhz, (iii) 800 Mhz y (iv) 2.6 Ghz.

(IV.1.) Banda de frecuencias de 900 Mhz[234].

En aplicación del principio de neutralidad tecnológica se amplían los sistemas que pueden utilizarse para prestar servicios de comunicaciones electrónicas, lo cual otorga más posibilidades a quienes explotan dichas frecuencias y por consecuencia se le establecen nuevas obligaciones.

Específicamente se señala que se podrán utilizar los sistemas de comunicaciones móviles digitales celulares públicos (GSM), los sistemas universales de telecomunicaciones móviles (UMTS) y otros sistemas terrestres capaces de prestar servicios de comunicaciones electrónicas que puedan coexistir con los sistemas GSM.

Por consecuencia, considerando que con la incorporación del principio de neutralidad tecnológica se ampliaron las posibilidades prestación, se dispuso que las empresas que explotaban dichas bandas, tuvieron, entre otras cosas, que: (i) revertir al Estado determinadas frecuencias; (ii) invertir en infraestructura o proporcionar nueva cobertura mínima de servicios con dicha infraestructura a fin de mantener el equilibrio económico – financiero de las concesiones demaniales, las cuales incrementaron su valor por la aplicación del principio de neutralidad tecnológica; (iii) ofrecer servicios mayoristas a los operadores que no puedan prestar servicios porque no tienen frecuencias o porque no tienen las suficientes.

Las condiciones para prestar los servicios mayoristas son acordadas libremente entre las partes, sin perjuicio la Comisión del Mercado de las Telecomunicaciones atenderá los conflictos que puedan surgir. Respecto del ER que sea revertido y que no estuviera asignado, se previó que se asignaría mediante concurso público.

[234] Artículo 4 del Real Decreto Nº 258/2011.

(IV.2.) Banda de frecuencias de 1800 Mhz[235]

En aplicación del principio de neutralidad tecnológica se autorizó a prestar servicios de comunicaciones electrónicas en dicha banda utilizando sistemas GSM, UMTS, así como otros sistemas terrestres que fueran capaces de prestar los servicios coexistiendo con los sistemas GSM.

En línea con lo anterior, se autorizó a las empresas que operaban dicha banda a poder hacerlo también utilizando otros sistemas que pudieran coexistir con los sistemas GSM. Por el otro lado, se les establecieron determinadas condiciones, como ser: revertir al Estado determinados bloques para mantener el equilibrio económico – financiero de las concesiones. Asimismo, se previó que los bloques que fueron revertidos, junto con otros que no habían sido asignados aún y que estaban disponibles, fueran asignados mediante concurso público, limitando la participación de los operadores que ya tuvieran asignados bloques de frecuencia en dicha banda.

(IV.3.) Banda de frecuencia de 800 Mhz[236]

A partir del año 2014 se previó su utilización para la prestación de servicios avanzados de comunicaciones electrónicas, la cual sería asignada por medio de subasta económica pública. Entre las condiciones se previeron: (a) concesiones demaniales, (b) la utilización de cualquier tecnología para prestar los servicios, (c) la finalización del término inicial de las concesiones al 31 de diciembre de 2030, (d) el desarrollo de un mecanismo de subasta simultánea ascendente de múltiples rondas, (e) el precio de salida de cada bloque de 5 Mhz apareado, (f) que los servicios que se presten no pueden causar interferencias para lo cual deben ajustar las características técnicas a las condiciones armonizadas. En caso de generar interferencias, deberán efectuar las correcciones técnicas necesarias para su eliminación, asumiendo los costes que fueren precisos para asegurar la continuidad del servicio.

(IV.4.) Banda de frecuencia de 2,6 Ghz[237]

Se prevé su asignación por medio de subasta económica pública, entre las condiciones se prevén: (a) concesiones demaniales cada una de 10 Mhz pareados, para comunicaciones ascendentes y descendentes en frecuencias diferentes, con un precio de

[235] Artículo 5 del Real Decreto Nº 258/2011.
[236] Artículo 6 del Real Decreto Nº 258/2011.
[237] Artículo 7 del Real Decreto Nº 258/2011.

salida de 10 millones de euros, (b) concesiones demaniales cada una de 5 Mhz pareados, para comunicaciones ascendentes y descendentes en frecuencias diferentes, con un precio de salida de 5 millones de euros, (d) la utilización de cualquier tecnología, (e) un plazo de vigencia específico, finalizando el 31 de diciembre de 2030, (f) la realización de una subasta simultánea ascendente de múltiples rondas.

V. El espectro radioeléctrico en la regulación de Uruguay

En Uruguay se define al ER como el *"conjunto de ondas radioeléctricas u ondas hertzianas, sin solución de continuidad, cuya frecuencia se fija convencionalmente en 3.000 ghz, que se propagan por el espacio sin guía artificial*".[238]

"*El espectro radioeléctrico es un patrimonio común de la humanidad sujeto a administración de los Estados y, por tanto, el acceso equitativo a las frecuencias de toda la sociedad uruguaya constituye un principio general de su administración."*[239].

"No existirá otra limitación a la utilización del espectro radioeléctrico que la resultante de establecer las garantías para el ejercicio de los derechos de todos los habitantes de la República, lo que define los límites y el carácter de la intervención estatal en su potestad de administrar la asignación de frecuencias.[240]"

El Estado administrará las frecuencias radioeléctricas, en base a los siguientes principios: (1) Promoción de la pluralidad y de la diversidad; (2) No discriminación, garantizando la igualdad de oportunidades; y (3) Transparencia y publicidad en los procedimientos y condiciones de otorgamiento de las asignaciones de frecuencias[241].

Uruguay aprobó por la Ley N° 16.303 la Constitución, el Convenio y el Protocolo Facultativo de la UIT,adoptados en la Conferencia de Plenipotenciarios de esta Organización, en la ciudad de Niza, el 30 de junio de 1989, así como la Reserva formulada por la República Oriental del Uruguay a dicho convenio; y por la Ley N° 16.967 aprobó las Enmiendas a la Constitución y al Convenio de la UIT adoptados en las Conferencias de Ginebra de 1992 y de Kyoto de 1994, así como la Reserva formulada por la República Oriental del Uruguay.

238 Artículo 3 del Reglamento de Administración y Control del Espectro Radioeléctrico, aprobado por el Decreto Nº 114/003.
239 Artículo 2 de la Ley N° 18.232 y artículo 9 de la Ley N° 19.307.
240 Artículo 1 de la Ley Nº 18.232 y artículo 9.2 de la Ley Nº 19.307.
241 Artículo 3 de la Ley Nº 18.232.

(V.1) Competencias de la administración en relación al ER

A la Dirección Nacional de Telecomunicaciones y Servicios de Comunicación Audiovisual (dinatel) le compete planificar la gestión del er[242]; y la Unidad Reguladora de Servicios de Comunicaciones (URSEC) tiene el cometido de administrarlo, defenderlo y controlarlo[243].

La administración, defensa y control, incluyen, entre otras funciones: (i) elaborar y aprobar planes generales de utilización; (ii) establecer las condiciones para el otorgamiento del derecho de uso y la comprobación técnica de emisiones radioeléctricas; (iii) inspeccionar estaciones y sistemas; (iv) la detección, localización, identificación y eliminación de irregularidades e interferencias perjudiciales para el correcto funcionamiento de los sistemas de telecomunicaciones; y (v) elaborar y aprobar los planes de utilización del ER,salvo los de radiodifusión los que serán elevados al Poder Ejecutivo para su aprobación.[244]

A fin de lograr la utilización coordinada y eficaz del ER,la URSEC aprobará el Cuadro Nacional de Atribución de Frecuencias, que establecerá las atribuciones de bandas, subbandas y canales radioeléctricos aplicables a las clases y categoría de servicios de radiocomunicaciones involucrados, así como las demás condiciones técnicas generales que pudieran ser necesarias.

Además, a la URSEC le compete:

i. otorgar autorizaciones precarias para el uso de frecuencias del ER nacional, así como para instalar y operar estaciones radioeléctricas, excepto las previstas para radiodifusión de amplitud modulada (am), frecuencia modulada (fm), televisión abierta y televisión para abonados.

ii. previa autorización genérica del Poder Ejecutivo, asignar el uso de frecuencias radioeléctricas por la modalidad de subasta u otro procedimiento competitivo.

En relación a los Servicios de Comunicación Audiovisual (sca):

1. Es competencia del Poder Ejecutivo:

242 Artículo 94 Bis, numeral 3, de la Ley Nº 17.296, agregado por la Ley Nº 18.719.
243 Artículo 86, literal c, de la Ley Nº 17.296.
244 Artículo 4 del Reglamento de Administración y Control del Espectro Radioeléctrico.

a. otorgar las concesiones, licencias y autorizaciones, requiriendo previo informe de URSEC cuando el servicio utilice ER o una red de telecomunicaciones propia;[245]

b. a través de Consejo de Comunicación Audiovisual, convocar a llamados públicos y abiertos a interesados en obtener una autorización o licencia para brindar sca, y la respectiva concesión de uso de ER en caso de corresponder.

c. Velar para que la utilización del ER sea realizada de la manera más eficiente posible, y que las concesiones se otorguen respetando sus limitaciones, los convenios internacional y su disponibilidad.[246]

d. Cambiar un canal radioeléctrico o las condiciones de funcionamiento autorizadas, incluyendo la disminución de espectro asignado, cuando sea necesario por convenios o acuerdos internacionales, cambios tecnológicos o motivos de interés general[247].

e. Asignar el canal de ER para la instalación y operación de estaciones de radiodifusión comunitaria, previo informe de URSEC y de la Comisión Honoraria Asesor de Radiodifusión Comunitaria.

f.Reservar, previo informe de URSEC y del Consejo Honorario Asesor de Radiodifusión comunitaria, para los servicios de radiodifusión comunitaria y otros sin fines de lucro, al menos un tercio del espectro radioeléctrico por cada localidad en todas las bandas de frecuencias de uso analógico y digital y para todas las modalidades de emisión.

2. Es competencia de URSEC:

a. Asesorar al Poder Ejecutivo y al Consejo de Comunicación Audiovisual en todo lo relativo a la utilización, control, fiscalización o supervisión del ER y los parámetros técnicos de operación de los sca que utilicen dicho recurso[248].

b. Fiscalizar, administrar, defender y controlar el uso del ER por parte de los sca[249].

245 Artículo 3, literal B, de la Ley Nº 19.307.
246 Artículo 88, inciso 2, de la Ley Nº 19.307.
247 Artículo 91 de la Ley Nº 19.307.
248 Artículo 65, literal A, de la Ley Nº 19.307.
249 Artículo 65, literal B, de la Ley Nº 19.307.

3. Es competencia del Consejo de Comunicación Audiovisual, previa autorización del Poder Ejecutivo, realizar los llamados públicos y abiertos a interesados en obtener una autorización o licencia para brindar sca y la respectiva concesión de uso de ER en caso de corresponder. Asimismo, para el otorgamiento de autorizaciones para radiodifusión comunitaria que utilicen ER,deberá expedirse previa y preceptivamente.

(V.2) Reglamento de Administración y Control del Espectro Radioeléctrico

Por medio del Decreto N° 114/003 se aprobó el Reglamento de Administración y Control del ER (racer), con el objeto de establecer las disposiciones que regirán la administración y el control del ER de dicho país.

A efectos del racer, "*se considera ER conjunto de ondas radioeléctricas u ondas hertzianas, sin solución de continuidad, entendiéndose por tales a las ondas electromagnéticas, cuya frecuencia se fija convencionalmente por debajo de 3.000 Giga Hertz que se propagan por el espacio sin guía artificial*.

El espectro radioeléctrico constituye un recurso natural y limitado del dominio público del Estado.

La utilización de ondas electromagnéticas de frecuencias superiores a 3.000 Giga Hertz y propagadas por el espacio sin guía artificial, tiene el mismo régimen que el de la utilización de las ondas radioeléctricas, siéndole de aplicación lo dispuesto en la Ley N° 17.296 y en el presente Reglamento".[250]

El racer parte de la base de que la administración, la defensa y el control del ER es imprescindible para propiciar su uso eficiente, así como para promover el desarrollo, la optimización y para la utilización de nuevos servicios radioeléctricos, redes y tecnologías.

El objeto del racer es establecer las disposiciones que regirán la administración y el control del ER nacional, y entre sus objetivos se encuentra[251]:

a. Usarlo de forma eficiente, procurando limitar el número de frecuencias y la extensión utilizada al indispensable para asegurar el funcionamiento satisfactorio de los servicios y sistemas.

b. Promover el uso como factor de desarrollo económico y social.

250 Artículo 3 del Reglamento de Administración y Control del espectro radioeléctrico.
251 Artículo 2 del Reglamento de Administración y Control del espectro radioeléctrico.

c. Propiciar el acceso equitativo, mediante procedimientos abiertos, transparentes y no discriminatorios.

d. Promover el desarrollo y la utilización de nuevos servicios radioeléctricos, redes y tecnologías y el acceso general a ellos, impulsando la aplicación a la mayor brevedad posible de los últimos adelantos de la técnica.

e. Contribuir a la planificación estratégica del sector de las telecomunicaciones.

La utilización del espectro radioeléctrico se debe hacer de acuerdo con la planificación que delimite las bandas y canales atribuidos a cada uno de los servicios y sistemas, conforme a lo establecido en el Cuadro Nacional de Atribución de Frecuencias y a lo establecido por otras normas específicas.

El Cuadro Nacional de Atribución de Frecuencias[252], es aprobado por la URSEC, establece las atribuciones de bandas, subbandas y canales radioeléctricos para cada clase y categoría de servicios, así como las condiciones técnicas, teniendo en cuenta: (i) el Reglamento de Radiocomunicaciones de la UIT,(ii) los Convenios Internacionales, (iii) las disposiciones nacionales e internacionales de canales radioeléctricos, (iv) las prioridades nacionales, (v) el privilegio en los usos del ER que sean de utilidad para el público o que sirvan para el desarrollo nacional, y (vi) la utilización futura de las distintas bandas de frecuencias.

Además, URSEC lleva el Registro Nacional de Frecuencias el cual contiene información sobre las asignaciones vigentes de frecuencias radioeléctricas y la conformación general de los sistemas que operan en ellas. El acceso al registro es público, salvo aquella información que por su naturaleza deba permanecer en reserva[253].

Los interesados en obtener autorización para el uso del ER deben presentar sus solicitudes ante la URSEC, quien según el tipo, características y modalidades del servicio de radiocomunicaciones de que se trate, determinará las formalidades y contenidos de la información a aportar por los interesados.

Sin perjuicio, en caso de que se deba acompañar un proyecto técnico, el mismo debe estar firmado por técnico competente en la materia de telecomunicaciones y

252 Artículo 5 del Reglamento de Administración y Control del espectro radioeléctrico.
253 Artículo 6 del Reglamento de Administración y Control del Espectro Radioeléctrico.

contener, como mínimo:[254] (a) Descripción de la estructura de la red o del sistema que se pretende instalar. b) Características técnicas de los equipos transmisores. c) Detalle del servicio a prestar, así como de las estaciones integrantes del sistema y de los emplazamientos de las estaciones fijas. d) Área de servicio, indicando lugares de emplazamientos previstos de los centros principales y secundarios del sistema. e) Detalle del requerimiento espectral con justificación de la banda, cantidad y carácter de la asignación solicitada. f) Cronograma para la instalación y puesta en funcionamiento. g) Expresión de conocimiento y conformidad a las disposiciones vigentes.

De considerarlo necesario, la URSEC puede implementar el procedimiento de consulta pública, a fin de que interesados puedan emitir su opinión y comentarios.

Asimismo, el racer le establece plazos máximos para resolver, sin perjuicio de que pueden ser extendidos para alcanzar la coordinación internacional que sea procedente. En caso de solicitudes cuya resolución no se encuentre supeditada a decisiones del Poder Ejecutivo, tendrá sesenta días corridos prorrogables por razón fundada; y en los supuestos de concesiones ligadas a procedimientos competitivos, se estará a lo dispuesto por el acto administrativo que apruebe el pliego de bases correspondiente.

Hay cuatro modalidades de uso del espectro radioeléctrico:

1. Uso libre: no requieren autorización de las estaciones ni asignación de frecuencia alguna. Son por ejemplo los sistemas de radiocomunicaciones de muy baja potencia. No deben producir interferencias perjudiciales, ni pueden pedir protección frente a otras estaciones que operen dentro de los parámetros autorizados.

2. Uso común: requieren autorización o permiso previo, no tienen asignación de frecuencia alguna. Son por ejemplo las frecuencias atribuidas a los servicios de radioaficionados, de socorro o de seguridad.

3. Uso específico: asociadas a determinados servicios o sistemas de radiocomunicaciones, requieren autorización con asignación de determinada frecuencia, sea con carácter compartido o exclusivo. Están asociadas a la prestación de un servicio de telecomunicaciones o a la instalación y operación de una red radioeléctrica propia.

254 Artículo 8 del Reglamento de Administración y Control del Espectro Radioeléctrico.

4. Uso general: no asociadas a servicio determinado o a sistema de radiocomunicaciones, requieren autorización con asignación de frecuencias con carácter exclusivo o compartido.

La utilización del ER debe realizarse de la manera *más eficiente posible.* Se entiende que se utiliza eficientemente cuando su uso es efectivo y continuo en las zonas geográficas para las que fue reservado, con un adecuado volumen de tráfico. No obstante, en el caso de sistemas destinados a la prestación comercial de servicios de telecomunicaciones, se podrá incluir como tal, la reserva espectral necesaria para el crecimiento previsible durante el período de vigencia del título habilitante correspondiente.

A la fecha el espectro radioeléctrico que se encuentra asignado espectro en las siguientes bandas de frecuencia: 700 MHz, 850 MHz, 900 MHz, 1700/1800 MHz, PCS, UMTS, AWS y AWS extendido, 2600 MHz.

Los parámetros de instalación y operación autorizados para operar el ER,tales como las frecuencias radioeléctricas, la potencia de radiofrecuencia de transmisión, el ancho de banda y otras características técnicas, son establecidos por URSEC y no deben ser modificados sin su previa autorización.

La potencia de radiofrecuencia radiada, no puede superar la autorizada y debe reducirse a la mínima necesaria compatible con el normal funcionamiento del sistema, pudiendo ser superada únicamente para comunicaciones de socorro.

Al respecto, vale destacar que el Decreto N° 53/2014 del Poder Ejecutivo, establece los límites para la exposición humana a los Campos Electromagnéticos (cem) y adopta como límites máximos permitidos los recomendados por la Organización Mundial de la Salud (oms) y contenidos en las Recomendaciones de la Comisión Internacional de Protección Contra las Radiaciones no Ionizantes (icnirp), sin perjuicio de las directivas y orientaciones complementarias de la oms y de la Organización Internacional del Trabajo (oit).

En lo que respecta a la asignación de frecuencias para el uso específico del ER,se deben respetar los siguientes principios: (a) Las frecuencias se deben asignar dentro de cada banda, conforme al Cuadro Nacional de Atribución de Frecuencias. (b) El área geográfica de la asignación será la de prestación del servicio, según corresponda. (c) Los titulares de las asignaciones que se otorguen deberán cumplir con las condiciones

que se les impongan en la resolución de autorización de uso del ER y las que correspondan a la licencia específica.

Las autorizaciones pueden ser: (a) sin plazo o permiso precario, otorgadas por URSEC, o (b) con plazo, también otorgadas por URSEC, con previa autorización genérica del Poder Ejecutivo.

Asimismo, deben contener, según corresponda, los siguientes aspectos: (a) los parámetros técnicos de funcionamiento, (b) el área de despliegue del sistema, (c) el carácter en que se asignan las frecuencias, (d) los plazos de vigencia y de puesta en funcionamiento.

Los derechos de usos específico y general del ER con prestación de servicios a terceros, cuando se trate de servicios de radiocomunicaciones ajenos a una licencia particular, se otorgan a demanda o mediante procedimientos competitivos.

En relación a los procedimientos competitivos, la URSEC puede promover la utilización de un Procedimiento Competitivo teniendo en cuenta: (i) la demanda de solicitudes de autorizaciones y (ii) la disponibilidad espectral.

En los casos en que se determine la utilización del Procedimiento Competitivo, la URSEC diseña el pliego y, cuando corresponda, lo eleva a consideración del Poder Ejecutivo.

Cuando se trate de frecuencias para los usos específicos y generales del ER necesarias para la instalación y operación de redes de uso propio, o cuando tratándose de frecuencias asignadas exclusivamente a servicios con prestación a terceros no se prevea escasez de frecuencias, las autorizaciones de uso específico o general del espectro radioeléctrico, se pueden otorgar a demanda.

Para poder transferir, arrendar o ceder las autorizaciones para instalar y operar estaciones, medios o sistemas radioeléctricos, así como las autorizaciones y permisos de uso de frecuencias del espectro radioeléctrico, se requiere autorización previa del Poder Ejecutivo o de la URSEC, según corresponda.

Podrá cancelarse la autorización en caso de que el ER no se esté utilizando en los términos y condiciones autorizados.

Por otra parte, el Poder Ejecutivo o la URSEC, según corresponda, podrán solicitar a los titulares de las autorizaciones y permisos de uso de frecuencias, la

migración de sus sistemas, si fuera necesario como consecuencia de cambios en el Cuadro Nacional de Atribución de Frecuencias. Ya sea por razones de interés público, de seguridad nacional, para la introducción de nuevas tecnologías, para solucionar problemas de interferencia perjudicial o para dar cumplimiento a acuerdos internacionales. En estos casos, la URSEC establecerá las condiciones y los plazos máximos para la migración, asignando las frecuencias de destino en las que se puedan ofrecer los servicios originariamente prestados.

VI. Consideraciones finales

El ER es un recurso natural, intangible, compartido, limitado, escaso, que se divide en bandas de frecuencias, a través de las cuales se transmiten las ondas electromagnéticas de los servicios de comunicación inalámbrica.

Es parte del dominio público de los Estados, quienes lo administran, gestionan y controlan a nivel nacional; pero la UIT,así como otros organismos regionales tienen un rol fundamental en la gestión, coordinación, armonización y compartición del ER a nivel mundial.

Es muy demandado y es imprescindible para la transformación digital, para la conectividad, para el acceso, para el desarrollo de los servicios inalámbricos, móviles y fijos, así como para el despliegue de redes de última generación; lo cual es esencial para disminuir la brecha digital, facilitar la innovación, promover la educación, universalizar nuevas tecnologías y desarrollar la economía digital.

En este contexto, la disponibilidad de espectro, el principio de neutralidad tecnológica y de servicios, así como la coordinación y compartición de recursos entre los diversos actores toman mayor relevancia; siendo primordial otorgar seguridad, reglas claras, dar previsibilidad, a fin de captar inversiones y promover el despliegue, haciendo los ajustes y las actualizaciones regulatorios que sean necesarias.

La regulación existente en España, a diferencia de la de Uruguay, parece reflejar en gran medidas la nueva realidad digital. La regulación en Uruguay debería ser analizada y actualizarse a efectos de facilitar el desarrollo y la innovación. El modelo seguido en España podría ser una buena guía a seguir para Uruguay.

CAPÍTULO V: SERVICIOS Y APLICACIONES DIGITALES

I. Introducción

Como hemos manifestado anteriormente[255], nos encontramos ante una revolución digital que viene a cambiar las estructuras políticas y socioeconómicas, que lo hace a través de Internet o en formato electrónico, y que se desarrolla a velocidad exponencial.

Esta revolución digital es consecuencia del gran desarrollo conjunto que han tenido las redes de telecomunicaciones y la tecnología, en tanto han facilitado que se generen nuevos servicios y soluciones digitales que atienden las necesidades de la sociedad, cambiando los modelos, utilizando los datos y generando una nueva economía.

Vivimos en la sociedad de la información, "*que viene determinado por la extraordinaria expansión de las redes de telecomunicaciones y, en especial, de Internet como vehículo de transmisión e intercambio de todo tipo de información. Su incorporación a la vida económica y social ofrece innumerables ventajas, como la mejora de la eficiencia empresarial, el incremento de las posibilidades de elección de los usuarios y la aparición de nuevas fuentes de empleo.*[256]"

En este sentido, como lo expresa Raúl Katz[257]*: "El desarrollo de las tecnologías de la información y de las telecomunicaciones y la convergencia tecnológica, tanto a nivel global como en América Latina, ha posibilitado el surgimiento de nuevos mercados de servicios y contenidos digitales, configurando un conjunto nuevo de interacciones entre los usuarios, las empresas del sector y los proveedores de dichos servicios". (...)*

"El ecosistema digital, entendido como el conjunto de prestaciones y requerimientos de diversa naturaleza que se proveen desde y a través de las redes de

255 ARAMENDÍA, MERCEDES, "La Revolución Digital: Telecomunicaciones, Servicios Digitales y la Sociedad de la Información" en *Estudios de Telecomunicaciones y Sociedad de la Información*, Universidad de Montevideo, 2018. Págs. 11 y ss.

256 Exposición de motivos de la ley N° 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.

257 KATZ, RAÚL: "El ecosistema y la economía digital en América Latina", agosto 2015, https://www.fundaciontelefonica.com/arte_cultura/publicaciones-listado/pagina-item-publicaciones/itempubli/430/

telecomunicaciones, el conjunto de infraestructuras y prestaciones asociadas que habilitan la prestación de dichos servicios, así como la interacción entre los prestadores de servicios de distinta naturaleza que constituyen la cadena de valor extendida de servicios de Internet, constituye un nuevo sujeto de análisis desde el que se debe pensar las políticas públicas. Este nuevo objeto de análisis ya ha comenzado a ser encarado recientemente por diversos entes y organizaciones internacionales."

En línea con lo anterior, considero que en esta revolución se presentan como claves los siguientes tres elementos:

1. el despliegue de redes de telecomunicaciones, para facilitar la conectividad, en tanto espina dorsal de todo esta nueva realidad;

2. el desarrollo de servicios y aplicaciones digitales, que se brindan a través de plataformas, que a su vez se despliegan sobre las redes de telecomunicaciones, impulsando la economía digital, que vienen a responder y a atender las necesidades de las personas; y

3. que los ciudadanos, las empresas y los gobiernos utilicen y confíen en las redes y en los servicios.

Las redes de telecomunicaciones son fundamentales para la prestación de los servicios y de las aplicaciones digitales, al tiempo que para que las redes de telecomunicaciones sean necesarias y se utilicen, se requiere de servicios y aplicaciones que se presten sobre las mismas. De esta manera, se entiende que dependen unos de los otros, pero lo que se presenta como realmente esencial es que los servicios, las aplicaciones y las redes se utilicen. Para esto es necesario que los ciudadanos, las empresas y los gobiernos hagan uso de los servicios, de las aplicaciones y por ende de las redes; para lo cual se les deben dar las garantías y seguridades necesarias para que confíen y se apalanquen en los mismos, haciendo el máximo uso de las tecnologías.

La sociedad y la economía digital plantean múltiples retos al orden establecido, en tanto modifican todos los ámbitos de nuestras vidas, siendo esencial que los ciudadanos, las empresas y los gobiernos nos adaptemos.

Los ciudadanos necesitamos desarrollar las competencias y habilidades digitales para poder ser parte de esta realidad, viendo protegidos y respetados nuestros derechos fundamentales. Las empresas deben poder producir y brindar sus servicios en igualdad de condiciones, con reglas de juego claras, previsibles. Los gobiernos deben responder,

otorgando transparencia, garantías y soluciones que atiendan las nuevas necesidades económicas y sociales, al tiempo que promuevan la innovación y el desarrollo de las redes de telecomunicaciones de última generación, así como de nuevos servicios y soluciones digitales. Lo anterior, debe ir acompañado de un análisis del ordenamiento jurídico actual, ajustar lo que sea necesario, desarrollar y modernizar lo que corresponda, teniendo siempre presente la velocidad de los cambios y los principios generales.

Hemos profundizado anteriormente sobre el despliegue de redes de telecomunicaciones, a continuación procederemos a desarrollar lo vinculado con los servicios y aplicaciones digitales.

II. Servicios y aplicaciones digitales

Los servicios y aplicaciones digitales se prestan a través de plataformas, que son softwares que se desarrollan –principalmente– sobre Internet y que brindan diversos servicios y soluciones.

Como señala la Comisión Europea en Comunicación al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones, com (2016) 288 final[258]: *"Las plataformas en línea han cambiado radicalmente la economía digital en las dos últimas décadas, aportando múltiples beneficios a la sociedad informática actual."*

Hay plataformas de diferentes formas y tamaños, se desarrollan constantemente y cubren las más diversas actividades: plataformas de publicidad en línea, mercados en línea, motores de búsqueda, redes sociales, medios de difusión de contenidos, plataformas de distribución, servicios de comunicación, sistemas de pago, plataformas dedicadas a la economía colaborativa, entre otros múltiples ejemplos[259].

Sin perjuicio de la gran variedad, se identifican ciertas características comunes:

1. Crean nuevos mercados y nuevas formas de hacer las cosas, disrumpiendo muchas veces en los mercados tradicionales.

258 Comunicación de la Comisión Europea, COM/2016/0288 final, URL https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A52016DC0288 Consultado el 20 de febrero de 2019.
259 Ibídem.

2. Generan nuevas formas de participar y de realizar negocios, principalmente en base a la recogida, almacenamiento y procesamiento de grandes cantidades de datos.

3. Están presentes en los más diversos mercados y áreas, de diferentes formas, presentando distintos tipos de servicios.

4. Se desarrollan en general sobre Internet, generando entornos virtuales, pero algunas complementan la prestación de los servicios o entrega de los productos con una parte física.

5. Generan mucha información a través de la interacción con las personas, lo cual se traduce en valor, en tanto facilitan la toma de decisiones y las estrategias.

Como resultado de lo anterior, han demostrado tener gran impacto social y económico. Lo vemos en las telecomunicaciones (por ejemplo en la sustitución que ocurrió con Whatsapp y los sms), en los servicios de transporte (por ejemplo con Uber o Cabify y el impacto en los taxis), en los servicios de alojamiento (por ejemplo con Airbnb y el impacto en los hoteles), en los servicios audiovisuales (por ejemplo con Netflix y el impacto en Blockbuster), en las fotografías digitales (por ejemplo con la tecnología en los celulares y el impacto en Kodak), entre otros múltiples ejemplos.

Cambian las formas y se han generado nuevos modelos de negocio[260]:

- Modelo de minoristas en línea: las plataformas en línea venden bienes o conectan a compradores y vendedores a cambio de una comisión por transacción o venta. Por ejemplo: Amazon o Mercado Libre.

- Modelo de medios sociales: los propietarios de las redes basan sus ingresos en la publicidad mediante el envío de mensajes comerciales específicos a los consumidores. Por ejemplo: Facebook o Instagram.

- Modelo de suscripción: las plataformas cargan cuotas de suscripción por el acceso ininterrumpido a diversos servicios digitales, como puede ser de música o de video. Por ejemplo: Spotify o Netflix.

260 Comunicación de la Comisión Europea Nº 547 del 21 de setiembre de 2017. URL: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX%3A52017DC0547&from=EN Consultado el 9 de diciembre de 2020.

- Modelo de plataforma colaborativa: las plataformas conectan la capacidad excedentaria de unos con la demanda de otros, utilizando mecanismos de reputación para apoyar el consumo y permitir a las personas compartir el acceso a los activos en lugar de poseerlos. Las plataformas cobran una comisión fija o variable sobre cada transacción. Por ejemplo: Airbnb o Blablacar.

  Este modelo también ha sido definido haciendo referencia al modelo de negocio en el que se facilitan actividades mediante plataformas, que crea un mercado abierto para el uso temporal de mercancías o servicios ofrecidos en algunos casos por particulares. Se presenta a tres categorías de sujetos: (1) prestadores de servicios, ya sean particulares o profesionales, que comparten activos, recursos, tiempos y/o competencias; (2) usuarios de dichos servicios; y (3) intermediarios que a través de las plataformas conectan a los prestadores con los usuarios y facilitan las transacciones[261].

Interesa destacar que estos nuevos modelos también suelen clasificarse según los sujetos que intervienen: consumidores, empresas y Administración Pública.

Como enseña la Profesora Susana Checa Prieto[262], los "consumidores" pueden ser tanto las personas que adquieren los bienes o servicios para su utilización final, como quienes los ofrecen, generalmente identificados por la letra "C" o "P" (por ejemplo: la conocida venta de garaje donde se produce el intercambio entre pares). Las "empresas" son aquellas que ofrecen o reciben productos o servicios, generalmente identificados por la letra "B". Finalmente, la Administración Pública, identificado por la letra "A" o "G". Las relaciones que se generen pueden ser de diversos tipos, generalmente se suele agregar un "2" en el medio para indicar que es entre ambos "*to*". En este sentido, se señalan las siguientes: (i) A2A: relaciones entre administraciones públicas, por ejemplo: solicitud de datos; (ii) A2B: relaciones entre una Administración Pública y una empresa, por ejemplo: notificación electrónica; (iii) A2C: relaciones entre una Administración Pública y un consumidor, por ejemplo: trámites en línea; (iv) B2A: relaciones entre una empresa y la Administración Pública, por ejemplo: declaración jurada; (v) B2B:

261 Comunicación de la Comisión Europea al Parlamento Europeo, al Consejo, al Comité Económico y al Comité de las Regiones: "Una Agenda Europea para la economía colaborativa" (Bruselas, junio 2016) (COM [2016] 356 final).

262 CHECHA, SUSANA, Profesora en el Máster de Acceso a la Abogacía, en Derecho Informático y Nuevas Tecnologías, de la Universidad de Nebrija, en el apartado "Comercio Electrónico".

relaciones entre empresas, por ejemplo: empresa y proveedor; (vi) B2C: relaciones entre empresa y consumidor, por ejemplo: una tienda virtual: y (vii) C2C o P2P: relaciones entre consumidores, por ejemplo: préstamos entre personas.

Actualmente con el gran desarrollo de la digitalización, también hay quienes hacen mención a dos nuevos actores fundamentales: los empleados, identificados con la letra ”E”, y los “Desarrolladores” de los servicios, identificándolos con la letra “D”. Tienen un rol fundamental para poder conectar a los diversos actores, generando relaciones con los Consumidores, con las Empresas y con los Gobiernos.

Por otra parte, también suele señalarse que esta nueva forma de relacionamiento puede ser completamente realizada por medios electrónicos o parcialmente, complementando la parte electrónica con los medios físicos tradicionales o viceversa. Asimismo, se suele hacer referencia al comercio electrónico directo u *on-line* cuando todo se produce por medios electrónicos, y al comercio electrónico indirecto u *off-line* cuando el objeto de la transacciones es tangible por lo que se perfecciona por los canales tradicionales. Finalmente, puede haber comercio electrónico abierto o cerrado. Es abierto cuando se perfecciona en redes públicas abiertas, y es cerrado cuando se requiere habilitación contractual previa[263].

Entre los principales sectores de actividad, en los que se ve el impacto de estos nuevos modelos se destacan: el alojamiento, el transporte de personas, servicios para la vivienda, servicios profesionales, técnicos, y de financiación colaborativa[264]; generando a su vez nuevos sectores de actividad como puede ser Legaltech (convergencia entre el Derecho y la Tecnología) y Fintech (el encuentro de las finanzas con la tecnología) que procedemos a comentar.

III. Legaltech

Como hemos señalado, gracias a la innovación, a la tecnología y a la conectividad, se han generado nuevos modelos, que impactan en múltiples industrias, como ser la forma en que se prestan los servicios profesionales y técnicos.

[263] CHECA, SUSANA, obra citada.

264 Surge de la nota al pie N° 1 de la Comunicación de la Comisión Europea (COM [2016] 356 final), en base a estimaciones de PwC Consulting en el marco de un estudio contratado por la Comisión Europea.

En este sentido, lo vemos por ejemplo en el Derecho y en los servicios jurídicos, con el desarrollo de Legaltech, en la Regulación, Regtech, en los Seguros, Insurtech, y lo vemos en la industria financiera, con el desarrollo de Fintech.

En lo que a los servicios jurídicos respecta, vemos cómo a través de la tecnología se simplifica el trabajo y la comercialización de los servicios legales. De esta manera, se permite que los abogados: (i) realicen su trabajo de una forma más eficaz y eficiente, haciendo uso de la tecnología, y (ii) brinden sus servicios a través de diversas plataformas electrónicas.

Lo anterior, por un lado beneficia a los abogados como prestadores de servicios, en tanto pueden hacer su trabajo de una mejor forma, al tiempo que pueden universalizar la oferta y la comercialización de sus servicios. Por el otro lado, también beneficia a los usuarios actuales y futuros de servicios legales, en tanto tienen más opciones de elegir, de comparar, así como de acceder a más variedad de servicios y a más información.

Entre las tecnologías que se consideran que más influirán en los servicios jurídicos se suele destacar a la Inteligencia Artificial (IA). Como enseña la Profesora Susana Navas Navarro: *"Un sistema de IA necesita de una secuencia de instrucciones que especifique las diferentes acciones que debe ejecutar el computador para resolver un determinado problema. Esta secuencia de instrucciones es la estructura algorítmica que emplea el sistema de IA. Por tanto, "algoritmo" es el procedimiento para encontrar la solución a un problema mediante la reducción del mismo a un conjunto de reglas"*[265] [266]

"Es común afirmar que el origen de la IA se encuentra en una conferencia sobre informática teórica que se celebró en Estados Unidos (Dartmouth College, 1956), a la que asistieron científicos que, poco tiempo después, dotaron a esta disciplina de una estructura teórica y computacional apropiada y la desarrollaron en diferentes ámbitos. Destacan John MCCARTHY, Marvin MINSKY, Allen NEWELL, y Hebert SIMON. Los dos últimos científicos mencionados presentaron, en aquella conferencia, un programa de ordenador, el Logic Theorist, que emulaba características propias del cerebro

[265] BENITEZ, R / ESCUDERO, G. / KANAAN, S. / MASIP RODÓ, D, Inteligencia artificial avanzada, editorial UOC, Barcelona, 2012, p. 13. Citado por NAVAS, SUSANA en ¨Derecho e inteligencia artificial desde el diseño¨ en *Inteligencia artificial. Tecnología. Derecho,* Tirant lo Blanch. Valencia. pp. 24.

[266] NAVAS, SUSANA, en obra citada, p. 24 y ss.

humano. Éste es considerado el primer sistema de inteligencia artificial que era capaz de demostrar los teoremas sobre lógica matemática expuestos en los tres volúmenes de los Principia Mathematica de Alfred N WHITEHEAD y Bertrand RUSSELL (1910-1913). Por su parte, los dos primeros científicos mencionados, John McCARTHY y Marvin MINSKY, fundaron más tarde el laboratorio de inteligencia artificial del MIT".[267]

"Se pensaba entonces que la IA tendría un gran impacto en el ámbito jurídico, pero no sucedió así, más bien lo contrario. La razón de ello venía principalmente del hecho de que el razonamiento basado en la lógica (logic-based knowledge and reasoning) no acababa de ser capaz de representar de forma adecuada las reglas legales, en la medida en que éstas pueden admitir diferentes interpretaciones, presentan ambigüedades, se redactan como cláusulas de carácter general, se emplean conceptos jurídicos indeterminados o pueden existir proposiciones jurídicas contradictoras y el razonamiento basado en la lógica se centra en afirmaciones de verdadero o falso sin apenas admitir matices. Asimismo, presenta otras limitaciones como que existan diferentes sistemas legales según las jurisdicciones o que las inferencias, en el método deductivo que emplea, no sean verdaderas, sino que presenten un mayor o menor grado de probabilidad de serlo existiendo siempre un margen de incertidumbre. El razonamiento jurídico no tiene que ser verdadero, sino que tiene que cumplir un determinado nivel de probabilidad. En el Derecho, se trabaja con "presunciones", lo que no deja de presentar sus dificultades para ser representadas por la lógica computacional clásica."[268]

Sin perjuicio, se ha avanzado en la automatización de los servicio jurídicos. *"Las actividades que pueden "automatizarse", gracias a los avances en IA, en el ámbito jurídico, son las siguientes: análisis, extracción de información relevante, predicción, generación de argumentos escritos o dialécticos, redacción de documentos contractuales, informes o memoranda, planificación de tareas en los despachos de abogados o en los juzgados, redacción de normas legales, análisis de tendencias en relación con cambios legales o doctrinales, o cambios de tendencias en los mercados que peritan pensar en un cambio en la estrategia inversora, predicciones, resolución de demandas mediante técnicas automatizadas de solución alternativa de conflictos,*

[267] NAVAS, SUSANA, en obra citada, p. 24 y 25.
[268] NAVAS, SUSANA, en obra citada, pp. 28.

control de calidad y aplicabilidad posterior a textos legales. A ellos, añadiría, la automatización del proceso de negociación de un contrato o la contratación mediante agentes inteligentes que tienen capacidad de autoaprendizaje y pueden tomar decisiones adaptadas al entorno".[269]

En esta línea, es interesante comentar algunos casos de innovación en la industria, diversas plataformas electrónicas que se han desarrollado y que atienden y/o facilitan los clásicos servicios legales. Vale destacar que lo anterior es posible gracias al desarrollo conjunto de la conectividad, la tecnología y la identificación de las necesidades del sector jurídico. Imaginemos que esto recién empieza, y en cuanto la oferta de las tecnologías de avanzada –como ser la inteligencia artificial, el desarrollo de algoritmos, almacenamiento en la nube, *big data*, blockchain, entre otros ejemplos– sea más accesible y asequible, el trabajo se facilitará cada vez más, permitiendo a su vez: optimizar los tiempos, disminuir errores, tomar decisiones más fundadas y resolver conflictos de una manera más simple y ágil.

Compartimos algunos ejemplos de aplicaciones y servicios:

- *Jurimetría*: es una plataforma basada en inteligencia artificial y *machine learning*, entre sus servicios ofrece: análisis de jurisprudencia, estadística y predictiva, permite tener más respuestas respecto a las posibilidades de éxito. Su página web es la siguiente: https://jurimetria.wolterskluwer.es/content/Inicio.aspx

- *Tirant Analytics*: es una plataforma que utiliza inteligencia artificial y *big data* para juristas, a fin de mejorar el tratamiento de las bases de datos y los resultados de las búsquedas. Su página web es la siguiente: https://analytics.tirant.com/analytics/

- *ross Intelligence*: es una plataforma de investigación legal, basada en inteligencia artificial para las leyes de los Estados Unidos, pudiendo ofrecer acceso a variada jurisprudencia. Su página web es la siguiente: https://rossintelligence.com

- *casetext*: es una plataforma que permite a los abogados prestar mejor sus servicios, accediendo a análisis de expertos, colaborando con mejorar la investigación legal y el acceso a leyes y reglamentos. Su página web es la siguiente: www.casetext.com

[269] NAVAS, SUSANA, en obra citada, pp. 34 y 35

- *Ravel Law*: es una plataforma que ofrece investigación analítica, una herramienta inteligente que combina búsqueda y análisis legal. Se basa en el conocimiento legal de expertos, en el aprendizaje automático y jurisprudencia de la Biblioteca de Derecho de Harvard. Su página web es la siguiente: https://home.ravellaw.com/

- *Lax Geex*: es una plataforma electrónica que automatiza la revisión de contratos. Su página web es la siguiente: https://www.lawgeex.com

Estos son solo algunos ejemplos que nos permiten visualizar cómo la industria del derecho va innovando, facilitando la prestación de los servicios y el acceso a los mismos. Cada vez hay más soluciones que facilitan realizar tareas repetitivas, como puede ser redactar o controlar contratos, buscar jurisprudencia y opiniones de expertos, resolver conflictos y ejecutar contratos de forma automática a través de contratos inteligentes o *smart contracts* y la tecnología *blockchain*.

Al respecto, interesa señalar que los Smart Contracts o contratos inteligentes, si bien comenzaron a ser utilizados en los años 90 por Nick Szabo para desarrollar protocolos entre terceros, acuñando la idea de aplicar la informática a los contratos para que sea más difícil incumplir, pero se han desarrollado con la tecnología blockchain, que permite –entre otras cosas- la realización de transacciones de forma automática, sin intermediarios, siendo el sistema quien controla y ejecuta.

Nick Szabo "*Definió el contrato inteligente como un conjunto de instrucciones, plasmadas en forma digital, que preverían protocolos que controlarían el cumplimiento. Su finalidad era utilizar instrumentos informáticos para conseguir que el incumplimiento fuera prohibitivamente costoso. Deberían poder cumplir los cinco objetivos básicos de los contratos en el Common Law: observabilidad (la posibilidad de que las partes puedan comprobar la ejecución de las prestaciones de sus contrapartes y acreditar la propia), verificabilidad (probar el cumplimiento o el incumplimiento), privacidad (conocimiento y control sobre el contenido y desarrollo del contrato) y ejecutabilidad. Igualmente destacaba que al diseñar los contratos inteligentes debería reducirse la intervención de intermediarios y terceros. Ha habido que esperar veinte*

años para que el desarrollo de la tecnología haya permitido hacer viable su propuesta[270]*".*

Los *smart contracts* tienen muchos beneficios, sobre todo en lo que respecta a los tiempos y a la seguridad del cumplimiento, en tanto una vez que se cumple la condición se ejecutan de forma automática. Sin perjuicio, presentan diversos desafíos con el ámbito jurídico. Destacamos: (i) Si una de las partes es la que configura el código, probablemente serán contratos de adhesión en tanto la otra parte no tenga posibilidades de negociar o de modificar las disposiciones, por lo que se tendrá que atender diversos aspectos, como por ejemplo que no haya cláusulas abusivas. (ii) Hay que atender que el consentimiento sea válido, en tanto menores e incapaces podrían estar contratando de esta manera, lo cual afectaría su validez. (iii) En caso de que se configure la nulidad del contrato o fuerza mayor que imposibilite el cumplimiento, se podrían generan múltiples problemas en tanto la tecnología blockchain es inalterable. (iv) Si se utilizan para bienes y servicios, en caso de que el consumidor quiera desistir de la compra, teniendo en cuenta que la blockchain es irreversible e inalterable, se podrían generar inconvenientes. (v) Considerando que la tecnología blockchain es descentralizada y distribuida, es muy difícil poder identificar a los responsables del tratamiento y procesamiento de los datos personales. (vi) Además es pública y transparente, por lo que diversos integrantes pueden acceder a la información, pudiendo afectar el consentimiento otorgado. (vii) Por otra parte, no es posible modificar o suprimir las transacciones que se realizaron, por lo que también se podrían estar vulnerando derechos de los titulares de los datos, como es el derecho al olvido.

Lo anterior, más allá de los desafíos planteados, resulta muy disruptivo y positivo, pero otro de los elementos que corresponde plantearse es qué pasa si hay un error en el sistema, cómo se distribuyen los riesgos, ¿hay que atender la culpa o son factores que exceden la culpa? ¿se configura caso fortuito?. Sobre el punto es interesante señalar lo que se menciona sobre la responsabilidad de los Robots: *"…debe plantearse, por un lado, la responsabilidad del poseedor de un robot u otro artefacto inteligente en el sentido de aplicar un régimen de responsabilidad objetiva y no por culpa y, por otro lado, del fabricante de éste, máxime cuando las máquinas se pueden comunicar entre ellas para llevar a cabo determinadas actuaciones frente a la detección de*

[270] GORRIZ, CARLOS, ¨Tecnología blockchain y contratos inteligentes¨ en *Inteligencia Artificial. Tecnología. Derecho*, Tirant lo Blanch, Valencia, pp. 188.

determinados fallos del sistema o de errores humanos. Aquí podría pensarse en diferenciar las clases de defectos para atribuir un régimen de responsabilidad u otro en función de aquéllos y no, simplemente, aplicar criterios de responsabilidad objetiva sin, en la norma, diferenciarlos. También podría aplicarse la regla de market share liability, como criterio de imputación objetiva, en la medida en que pueda haber incertidumbre subjetiva en la causación del daño"[271].

Finalmente, otro elemento que genera desafíos es lo vinculado a la jurisdicción aplicable, al ser la tecnología blockchain virtual y descentralizada, puede ocurrir que las partes estén en diversos países y además que la legislación sea diferente o incluso contradictoria. Sin duda aún falta mucho por desarrollar, es importante ir identificando los diversos retos y contradicciones que pueden surgir respecto a las regulaciones actuales, a fin de ir buscando soluciones que faciliten la universalización de la tecnología en un todo conforme a los derechos fundamentales.

La tendencia de la prestación de los servicios apunta a la automatización, pero como viene de señalarse al comentar sobre los smart contracts, las oportunidades que presentan las nuevas tecnologías, también conllevan desafíos, en tanto las mismas permiten identificar tendencias, detectar patrones de conducta en las sentencias, así como analizar resultados, trayectoria, argumentos y diversos posicionamiento de los jueces.

Ante esta nueva realidad Francia en la nueva Ley de Reforma de la Justicia dispuso en el artículo 33 que "*Los datos de identidad de los magistrados y miembros del Registro no pueden ser reutilizados con el propósito o el efecto de evaluar, analizar, comparar o predecir sus prácticas profesionales reales o presuntas*[272]" .

Estos grandes cambios recién comienzan, sin duda la posición tomada por Francia parecería ser contraria a la tendencia, así como al buen uso que se puede dar a las

---

[271] NAVAS, SUSANA, GORRIZ LOPEZ Y OTROS, *Inteligencia artificial. Tecnología. Derecho*, Tirant lo Blanch, Valencia, 2017.

[272] Traducción propia de: *"Les données d'identité des magistrats et des membres du greffe ne peuvent faire l'objet d'une réutilisation ayant pour objet ou pour effet d'évaluer, d'analyser, de comparer ou de prédire leurs pratiques professionnelles réelles ou supposées. La violation de cette interdiction est punie des peines prévues aux articles 226-18,226-24 et 226-31 du code pénal, sans préjudice des mesures et sanctions prévues par la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés."* URL: https://www.legifrance.gouv.fr/jorf/article_jo/JORFARTI000038261761?r=oroM9UAyOR Consultado el 10 de junio de 2019.

herramientas tecnológicas, dando más transparencia y previsibilidad al trabajo del Poder Judicial.

Por otra parte, así como se comienza a hablar de la necesidad de que los contratos dejen de escribirse para pasar a ser programados, para lo cual va a ser fundamental poder comprender: lenguaje jurídico, tecnológico y de programación, también como indica Lawrence Lessig se hace énfasis que "*code is law*", lo cual implica que además de entender el mundo real en que vivimos, también debemos poder comprender el código del mundo digital.

Como clara muestra de que esta tendencia se va a profundizar cada vez más, interesa destacar que Uruguay, junto con Nueva Zelanda e Israel, comunicaron a fines del 2018 que están trabajando en el proyecto "Legislación como código" (*Legislation as code*), que busca traducir leyes a código informático, lo que permitiría que las máquinas las puedan procesar, facilitando muchas tareas[273].

Asimismo, interesa destacar que, según se ha difundido, "*Estonia se ha convertido en el primer país del mundo en proponer oficialmente la creación de un juez robot que sirva para descongestionar los juzgados del país. Y el encargo no ha recaído ni en juristas de reconocido prestigio ni en abogados con años de experiencia en el sector legal. El responsable del proyecto será Ott Velsberg, informático de profesión que ostenta el cargo público de responsable de datos de Estonia.*

Eso no quiere decir que no se tenga en cuenta la opinión de los expertos en el mundo del derecho, pero sí pone de manifiesto la complejidad a la hora de encontrar perfiles profesionales donde han de confluir conocimientos hasta ahora propios de profesiones diferenciadas: abogado, ingeniero, informático, gestor de procesos, economista…[274]"

Interesa concluir con la siguiente reflexión que resulta impactante y bien diferente a lo que venimos acostumbrados: *¨La IA, la tecnología en la que se basa, el Derecho que la regula y el Estado que lo produce, pueden reforzarse mutuamente, pueden retroalimentarse, pueden condicionarse en aras a un mayor bienestar y una mejor*

273 AGESIC, URL: https://www.agesic.gub.uy/innovaportal/v/7575/1/agesic/uruguay-nueva-zelanda-e-israel-crean-prototipo-para-traducir-leyes-a-codigo-informatico.html Consultado el 25 de febrero de 2019.

274 EXPANSION: "Diez tendencias que marcan el futuro del sector legal". URL: https://www.expansion.com/juridico/actualidad-tendencias/2019/04/15/5cb0a8a122601d8f358b45c6.html Consultado el 29 de abril de 2019.

calidad de vida humana y animal. Al cabo, un nuevo orden jurídico basado en (pocos) principios generales del Derecho cuya aplicación práctica se haga a través de códigos de conducta o deontológicos sectoriales, puesto que valores morales como la salud, la seguridad, la privacidad, la dignidad humana, la justicia, la no discriminación o la sostenibilidad del medio ambiente, deben merecer una especial atención, para mantener dentro de sus ¨justos¨ y ¨necesarios¨ límites al ¨algoritmo¨ reflejado en el ¨código binario¨ que puede acabar imponiéndose como, en su momento, vaticinó LESSIG, como forma de regular, modelar y dirigir el comportamiento humano".[275]

En suma, esto es solo el comienzo y tiene muchos beneficios, entre los cuales destacamos: menos errores, más conexión, más coordinación, menos costos, más accesibilidad, más predicción, más rapidez, más transparencia, al tiempo que permite concentrarnos en las estrategias, en la creatividad y en la relación con el cliente; lo subjetivo es menos sustituible.

IV. Fintech

Se le denomina de esta forma a la unión entre las finanzas y las tecnologías, implica el desarrollo de diversas plataformas tecnológicas que brindan servicios y/o soluciones financieras, facilitando que la industria sea más innovadora e inclusiva.

Al respecto, el Jefe de la División de Conectividad, Mercado y Finanzas del Banco Interamericano de Desarrollo indicaba que "*Los distintos desarrollos tecnológicos que han tenido lugar durante la última década en el mundo, junto con los nuevos modelos de negocio que estos han generado, están alterando el statu quo de la industria de los servicios financieros. Hoy es imposible analizar el sector sin tener en cuenta el impacto de las nuevas tecnologías financieras y de los emprendedores o compañías "fintech" que las implementan. Son estos los nuevos actores que compiten con las instituciones financieras tradicionales y desafían sus largamente establecidos modelos de negocio. Y aunque todavía se discute si la trasformación del sector tendrá lugar por la vía de la competencia o más bien de la colaboración entre unas y otras, los cambios que conlleva esta revolución tecnológica no tienen marcha atrás.*

[275] ¨The Zones of Cyberspace¨, 1996, Stanford LR, pp. 1403-1408, Code and Other Laws of Cyberspace, New York: Basic Books, 1999, pp. 53-54: LEENES, R., ¨Framing Techno-Regulation: An Exploration of State and Non-state Regulation by Technology", Tilburg Law School Legal Studies Research Paper Series n. 10/2012, http://ssrn.com/abstract=2182439. Fecha de consulta: octubre de 2017. Citado por NAVAS, SUSANA en obra citada, pp. 48 y 49

Afortunadamente esta dinámica de cambios imparables constituye una serie de buenas noticias para América Latina.[276] ”

Como surge del Informe Fintech realizado por el bid y Finnovista en el año 2017, se han desarrollado una gran variedad de soluciones y plataformas, permitiendo que consumidores, pymes[277] e instituciones financieras puedan acceder a un mayor número de servicios financieros y a mejores condiciones para gestionar sus finanzas o negociar sus activos.

Se han generado múltiples soluciones y plataformas que, haciendo uso de la tecnología, facilitan el acceso a los servicios financieros, en mejores condiciones, en tanto atienden sectores específicos del mercado y procuran hacerlo en condiciones más competitivas.

De esta forma se está buscando atender el GAP que hay entre las ofertas tradicionales y las necesidades de las personas, apalancándose en la tecnología; pero los nuevos servicios y soluciones que se plantean tienen desafíos, siendo la regulación un factor que facilitará y diferenciará a los países: aquellos que entiendan, atiendan y promuevan la nueva realidad, con una visión cabal, desarrollarán mejor el ecosistema generando más oportunidades para todos.

Es esencial nutrirnos, aprender de las experiencias que ya tienen otros países -que ya tienen más camino transitado en la temática- para poder responder de una manera más inteligente, adecuada, evitando errores, ateniendo la necesidad y la realidad, de una manera proporcionada. El trabajo en conjunto, el entendimiento y el diálogo entre los diversos actores del sector, medir, controlar, así como revisar periódicamente las soluciones propuestas y dictadas, es fundamental.

Hay múltiples tipos de soluciones y plataformas FINTECH[278], destacamos las siguientes:

1. Plataformas de Financiación Alternativa: Hay diversas modalidades, por ejemplo: (i) Financiación colectiva por recompensa: a través de plataformas las personas aportan recursos financieros a individuos, a proyectos o a compañías a cambio

276 BID y Finnovista. Fintech: Innovaciones que no sabías que eran de América Latina y Caribe. Año 2017. URL: https://publications.iadb.org/es/fintech-innovaciones-que-no-sabias-que-eran-de-america-latina-y-caribe Consultado el 9 de diciembre de 2020.

277 Pequeñas y Medianas Empresas.

278 BID y Finnovista, obra citada.

de productos o recompensas no monetarias. (ii) Financiación colectiva de donaciones: similar a la anterior, con la diferencia de que aportan por motivos filantrópicos y sin expectativas de un retorno monetario o material. (iii) Financiación colectiva de capital: plataformas mediante las cuales las personas adquieren participación accionaria. (iv) Préstamos en balance a consumidores o a negocios: plataformas operadas por entidades que proveen préstamos en línea a personas o a empresas. (v) Préstamos P2P a consumidores o a negocios: Plataformas a través de las cuales personas proveen préstamos en línea a personas o a empresas. (vi) *Factoring* y préstamos de facturas: plataformas en línea donde personas o entidades compran facturas o cuentas por pagar de otros negocios u ofrecen préstamos respaldados por ellos.

2. Puntaje alternativo (*Scoring*): Soluciones para medir el riesgo crediticio de personas o empresas.

3. Soluciones de pago: (i) Pagos y carteras móviles: soluciones móviles para la transmisión y administración de dinero. (ii) Transferencias internacionales y remesas: soluciones en línea diseñadas para el envío de dinero a empresas o a personas en el extranjero. (iii) Puntos de venta móviles: a través de los celulares. (iv) Pasarelas y agregadores de pagos: soluciones para la aceptación, autorización y procesamiento de pagos en plataformas digitales. (v) Soluciones con criptomonedas.

4. Gestión de finanzas personales: (i) Ahorro y eficiencia financiera: herramientas digitales para consumidores que facilitan la gestión de ahorro y la organización de gastos. (ii) Plataformas de comparación: plataformas que contrastan diferentes productos financieros y sus características. (iii) Gestión de deuda: colaboran con consumidores para la gestión y reestructuración de deudas.

5. Gestión de finanzas empresariales: (i) Facturación electrónica. (ii) Contabilidad Digital. (iii) Gestión financiera, inteligencia de negocio. (iv) Cobranzas.

6. Empresas de tecnología para instituciones financieras: (i) Seguridad e Identidad Digital: soluciones de verificación y autentificación de personas para acceso y autorización. (ii) Soluciones de identidad y conocimiento del cliente (kyc). (iii) Prevención de fraude y gestión de riesgo: Soluciones enfocadas en la prevención de fraude. (iv) Biométricos: Aplicaciones para verificar la identidad a través de los rasgos físicos. (v) Contratos inteligentes: protocolos que aseguran y ejecutan acuerdos.

7. Gestión patrimonial: (i) Gestión patrimonial digital: oferta y provisión de servicios de gestión. (ii) Asesores robotizados: soluciones automatizadas a través de algoritmos y de inteligencia artificial.

8. Negociación de activos financieros (*trading*) y mercado de valores: compra y/o venta de divisas extranjeras, compraventa de acciones y deuda, transacciones de otras clases de activos

9. Bancos Digitales: entidades financieras de nueva creación, con productos financieros, cuya distribución es 100 % digital.

Según surge del informe Fintech del año 2018[279], los tres segmentos que se presentan como los más representativos en América Latina son: (i) pagos y remesas, (ii) préstamos, y (iii) gestión de finanzas empresariales. Lo anterior lo explican por la masificación de los dispositivos móviles, las altas tasas de población subatendida y/o excluida del sistema financiero formal, así como por las limitaciones en la oferta por parte de los actores financieros tradicionales.

Vale destacar que al compararse el informe del año 2017 con el del año 2018, se ve un crecimiento en los emprendimientos relacionados con puntaje crediticio, identidad y fraude –lo cual muestra la importancia de los aspectos relacionados con ciberseguridad– y con banca digital –lo cual se explica con la necesidad de ofrecer productos y servicios que atiendan a las nuevas generaciones, y por la importancia creciente de los dispositivos móviles–[280].

El segmento de pagos y remesas es el que tiene mayor auge, lo cual va en línea con el alto índice de población excluida del sistema financiero tradicional –solo el 51 % de la población adulta tiene acceso a una cuenta en una institución financiera–, y con la elevada penetración de dispositivos móviles en la región –alrededor del 67 % según gsma, 2018–. Dentro de este segmento, se han potenciado: (i) pasarelas y agregadores de pago: que muestran la necesidad de dar soluciones de pago menos costosas y eficientes; (ii) soluciones que permiten pagos móviles y billeteras electrónicas: que reflejan el auge de realizar transacciones y transferencias de dinero entre personas, así como de comprar productos y/o servicios a través del celular o transacciones con

279 BID y Finnovista. Fintech América Latina 2018. Crecimiento y Consolidación. URL: https://publications.iadb.org/es/fintech-america-latina-2018-crecimiento-y-consolidacion Consultado el 9 de diciembre de 2020.
280 BID y Finnovista, obra citada.

tarjetas de débito o crédito; (iii) otros tipos de soluciones que incluyen plataformas de transferencias internacionales y remesas, soluciones de pago móvil en puntos de venta y soluciones con criptomonedas[281].

Europa tiene más camino transitado en la temática y los bancos tradicionales han jugado un rol fundamental como principales inversores, contribuyendo para crear el mercado único digital[282]. Además, las regulaciones vienen siendo analizadas y actualizadas constantemente, al tiempo que se procura atender la nueva realidad digital, trabajando sobre todo el ecosistema y siendo conscientes de que la digitalización no conoce fronteras.

En relación a las "criptomonedas", el Diccionario de Oxford define a las "criptomonedas" como una moneda digital donde técnicas de encriptación son usadas para regular la generación de unidades de monedas, así como para verificar la transferencia de fondos, operando de manera independiente de un banco central[283].

El uso de las criptomonedas se ha difundido mucho en los últimos diez años, siendo *Bitcoin* la más conocida y *Blockchain* (o cadena de bloques) la tecnología que se utilizó para desarrollarla.

Bitcoin fue la primer criptomoneda, se creó en el año 2008 por Satoshi Nakamoto quien explica en detalle el funcionamiento en el "*Bitcoin Paper*", donde define –entre otras cosas– a la moneda electrónica como una cadena de firmas electrónicas, que no depende de la confianza de una entidad central, que crea una red de usuario a usuario, que registra una historia pública de transacciones, distribuida, encriptada, irresoluble y que no puede ser modificada.

En el año 2009 la tecnología *Blockchain* comenzó a tomar valor, se empezaron a desarrollar nuevas criptomonedas y a desplegar otras aplicaciones, como ser: mejorar el control en las compras estatales, optimizar las cadenas de suministros, desarrollar *smart*

---

281 Ibídem.

282 BBVA en "¿Cómo se ha regulado la experiencia "fintech" en Eruopa?" URL: https://www.bbva.com/es/ha-regulado-experiencia-fintech-europa/ Consultado el 20 de julio de 2019.

283 Diccionario de Oxford, definición de "cryptocurrency". URL https://www.lexico.com/definition/cryptocurrency (Traducción propia: A digital currency in which transactions are verified and records maintained by a decentralized system using cryptography, rather than by a centralized authority.
'decentralized cryptocurrencies such as bitcoin now provide an outlet for personal wealth that is beyond restriction and confiscation').

contracts (o contratos inteligentes), así como para automatizar y simplificar muchos procesos.

Muchos países están trabajando en la regulación de las criptomonedas y especialmente en relación a su tecnología, en tanto permite transmitir valor de forma digital, sin tener que confiar en una entidad central.

Hay diversas posiciones respecto a cómo regularlo, pero en general se reconoce como una representación digital de valor, que se puede intercambiar por bienes y servicios.

En Estados Unidos, *The Uniform Law Commission* (ULC) definió a las monedas virtuales como una representación digital de valor que se usa como medio de intercambio, unidad de cuenta o como un almacén de valor, que no es moneda de curso legal. Excluyen expresamente las transacciones que son programas de recompensas para comerciantes, si el valor no se puede cambiar por moneda de curso legal, crédito bancario o moneda virtual; y representaciones digitales de valor emitidas por un editor y que se utilizan únicamente dentro de un juego en línea o plataforma de juego[284].

La Unión Europea define a las monedas virtuales como *"representación digital de valor no emitida ni garantizada por un banco central ni por una autoridad pública, no necesariamente asociada a una moneda establecida legalmente, que no posee el estatuto jurídico de moneda o dinero, pero aceptada por personas físicas o jurídicas como medio de cambio y que puede transferirse, almacenarse y negociarse por medios electrónicos"* y a los *"proveedores de servicios de custodia de monederos electrónicos"* como *"una entidad que presta servicios de salvaguardia de claves criptográficas privadas en nombre de sus clientes, para la tenencia, el almacenamiento y la transferencia de monedas virtuales."*[285].

Como reconoce el Banco Central Europeo, las monedas digitales *"no tienen que cambiarse necesariamente por monedas legalmente establecidas, sino que pueden también utilizarse para adquirir bienes y servicios sin necesidad de cambiarse por monedas legalmente establecidas o recurrir a un proveedor de servicios de custodia de*

284 BURR & FORMN LLP: Uniform Regulation of Virtual-Currency Businesses Act Offers States Regulatory Framework for the Virtual Currency Industry. URL: https://www.lexology.com/library/detail.aspx?g=35b99670-7c77-4db6-8b69-53ce4ec21410 Consultado el 25 de febrero de 2019.

285 Directiva (UE) 2018/843 del Parlamento Europeo y del Consejo de 30 de mayo de 2018.

monederos electrónicos", además, "*reconoce que los avances tecnológicos que presenta la tecnología de registros distribuidos subyacente a medios de pago alternativos como las monedas virtuales tienen el potencial de incrementar la eficiencia, el alcance y la variedad de los métodos de pago y transferencia. Sin embargo, los órganos legislativos de la Unión deben evitar aparecer como impulsores del uso de monedas digitales establecidas con carácter privado, pues estos medios de pago alternativos ni están legalmente establecidos como monedas ni son monedas de curso legal emitidas por bancos centrales y otros poderes públicos.*[286]"

Por su parte, *blockchain* es una base de datos, distribuida entre diversos participantes, organizada como una cadena de bloques, protegida criptográficamente, que no pueden ser alterada, que mantiene un consenso que verifica y confirma las transacciones, haciéndolas irreversibles.

Los elementos básicos de una *blockchain* son[287]: (1) Nodos: son ordenadores que forman una red, todos poseen el mismo software o protocolo que les permite conectarse y comunicarse entre sí. (2) Protocolo estándar: para que los nodos que forman la red se comuniquen entre sí, validen y almacenen la información registrada en la red. (3) Red entre pares: red de nodos conectados directamente. (4) Sistema descentralizado: no hay una jerarquía entre los nodos, todos son iguales entre sí.

Hay distintos tipos de *blockchain*: públicas, privadas y también las híbridas.

En las públicas, cualquiera puede acceder, son abiertas, descentralizadas, todos los nodos son iguales, no se controla quienes participan, los propietarios no son identificables personalmente, aunque sus direcciones pueden ser rastreables. Las unidades que se utilizan para representar un registro suelen denominarse "*tokens*". El ejemplo más conocido, la red de *bitcoin* –en la misma juega un gran rol la minería y la prueba de trabajo (pow)–, pero no todas tienen la misma operativa.

Las privadas son cerradas, aunque se pueden establecer diversos niveles de acceso, no toda la información en la *blockchain* es accesible o puede ser consultada. Son

286 Dictamen del Banco Central Europeo, de 12 de octubre de 2016, sobre una propuesta de directiva del Parlamento Europeo y del Consejo por la que se modifica la Directiva (UE) 2015/849 relativa a la prevención de la utilización del sistema financiero para el blanqueo de capitales o la financiación del terrorismo, y por la que se modifica la Directiva 2009/101/CE (CON/2016/49).

287 TAPSCOTT, Don: *La Revolución Blockchain.* Deusto, Barcelona, 2017, págs. 55 y ss.

distribuidas, se reparten entre varios nodos, aunque el número de nodos puede estar limitado. Además, se puede establecer el nivel de anonimato. Uno de los ejemplos más conocidos es Ripple, es abierto pero para las conversiones de divisas se debe estar previamente autorizado. Otras conocidas son las ofrecidas por la Fundación Linux. Las *blockchain* privadas suelen desarrollarse en el sector financiero (o regulados) por la imposibilidad de compartir determinados datos de forma abierta, se les suele denominar *Distributed Ledger Technology* (dlt) o Tecnología del Libro Mayor Distribuido.

Las híbridas, toman características de una y otra.

En definitiva, se entiende que a través de las Fintech se puede trabajar sobre clásicos problemas de la industria financiera como ser: la brecha de financiamiento, los costos transaccionales, las dificultades para acceder al crédito, los tiempos, la seguridad y los fraudes.

En este sentido, están en constante crecimiento y entre las tendencias se presentan las siguientes: (1) Usar las tecnologías móviles, sin tener que ir físicamente al banco. (2) Bancos cada vez más digitales. (3) Tecnología biométrica, para luchar contra los ciberataques y contra los fraudes, al tiempo que facilita acceder a los servicios. (4) Tecnología Blockchain para dar transparencia y para el desarrollo de contratos inteligentes que pueden automatizar las operaciones financieras. (5) Inteligencia Artificial, automatizan el análisis de los datos, monitorean tendencias y conductas, detectan fraudes, utilizan *chatbots* y asesores robots[288].

Entre las principales dificultades que se identifican para el desarrollo de la industria, considerando las repercusiones que la industria financiera tiene en la sociedad y en la economía, se plantea la necesidad de marcos regulatorios que otorguen seguridad y permitan su consolidación y crecimiento.

En el informe Fintech del año 2017, se señala la importancia de atender las buenas prácticas que puedan fomentar el desarrollo del sector, en tanto regulaciones restrictivas pueden impedir que se pueda operar. Para impedir esto, se recomienda que los reguladores compartan con los diversos actores las iniciativas y proyectos reglamentarios o legislativos, a fin de alcanzar soluciones que promuevan la innovación,

288 QUORA: "Everything you need to know about the top five Fintech trends of 2018". URL: https://www.forbes.com/sites/quora/2018/09/25/everything-you-need-to-know-about-the-top-five-fintech-trends-of-2018/#35798c666b93 Consultado el 20 de febrero de 2019.

fomenten la inversión, generando impactos sociales positivos, así como reduciendo la exclusión financiera[289].

Asimismo, se hace mención de que en el año 2016 el bid publicó un documento titulado: *"Alternative Finance (Crowdfunding) Regulation in Latin America and the Caribbean: A Balancing Act"*, donde se explican los modelos existentes de financiación colectiva, se hacen recomendaciones para que se expida una regulación balanceada y se destacan buenas prácticas implementadas en otros países, como en Reino Unido y Singapur. En dichos países, se dieron exenciones temporales sobre las autorizaciones para las Fintech y además se crearon bancos de prueba regulatorios temporales (conocidos como *sandbox*), en los que las Fintech puedan operar, evaluar sus modelos de negocio y ofrecer productos innovadores en ambientes monitorizados, controlados por el Regulador. Otra tendencia favorable, es la creación de algún tipo de institucionalidad dentro del sector público que sirva de interlocutor entre la industria y los responsables por la formulación de políticas.[290]

En el Informe Fintech correspondiente al año 2018, en relación a la regulación, se hace referencia a que las Fintech están desafiando a la industria financiera tradicional, con modelos de negocios innovadores y nuevos canales que prestan más variedad de servicios a los consumidores. Asimismo, se señala que los gobiernos son conscientes del potencial que tienen para el desarrollo de la economía, por la reducción de costos, el aumento de la competitividad y de la inclusión financiera. Finalmente, se hace énfasis en la importancia de trabajar en políticas y regulaciones que permitan el crecimiento de la industria al tiempo que haya supervisión adecuada.

En vista de lo anterior, se destaca la Ley Fintech de México como un ejemplo sobre cómo abordar la regulación desde una perspectiva proporcional e integral. Asimismo, se indica que el objetivo fue ofrecer una mayor certeza jurídica a través de un marco legislativo para regular las plataformas denominadas Instituciones de Tecnología Financiera (itf), así como establecer un marco que asegure una competencia justa entre los emprendimientos Fintech y las instituciones financieras y bancarias tradicionales. Señalan que se enfoca principalmente en cuatro áreas: 1. Instituciones de Tecnología Financiera (itf), compuestas por compañías financieras de *crowdfunding* e instituciones de pago electrónico; 2. Activos virtuales (criptomonedas); 3. Interfaces de

289 BID y Finnovista en el Informe Fintech del año 2017, obra citada.
290 BID y Fnnovista, obra citada.

programación aplicadas (api); y 4. Autorizaciones temporales para pruebas de innovación (*sandboxes*), para entidades previamente reguladas y para Fintech, por separado[291].

Asimismo, es de interés destacar la Directiva (ue) 2015/2366 del Parlamento Europeo y del Consejo del 25 de noviembre de 2015 sobre servicios de pago en el mercado interior (conocida como "psd2"), que busca desarrollar un mercado de pagos electrónicos seguro para apoyar el crecimiento de la economía, para garantizar las posibilidades de elección y para establecer condiciones de transparencia en los servicios de pago.

Como surge de la exposición de motivos, entre otras cosas: (i) Se parte de la base de que el mercado de pagos minoristas ha experimentado notables innovaciones técnicas, que han dado lugar a un rápido incremento del número de pagos electrónicos y de pagos móviles, y a la aparición de nuevos tipos de servicios de pagos en el mercado. (ii) Importantes sectores de mercados de pagos están fragmentados según las fronteras nacionales y muchas de las reglamentaciones son obsoletas o ambiguas, no reflejan la evolución del mercado; todo lo cual genera inseguridad jurídica, riesgos en la cadena de pago y desprotección del consumidor. (iii) Se necesita claridad jurídica, aplicación uniforme del marco regulador, garantizando condiciones operativas equivalente, tanto a los operadores existentes como a los nuevos, para lo cual la definición de servicios de pagos debe ser tecnológicamente neutra y permitir el desarrollo de nuevos tipos de servicios de pago, garantizando condiciones operativas equivalentes. (iv) Hay que facilitar que los nuevos medios de pago lleguen a un mayor número de consumidores, asegurando su protección en el uso de los servicios. Quedan fuera del objeto de la norma, entre otros, los pagos efectuados en efectivo y por medio de cheques en papel. (v) Se reconoce que disponer de servicios de pago fiables y seguros es esencial para el buen funcionamiento del mercado de servicios de pago, así como para el mantenimiento de actividades económicas y sociales.

En definitiva, como ha comunicado la Comisión Europea en comunicado de prensa[292], con los cambios que prevé la psd2 se pretende responder a la realidad actual

291 BID y Finnovista, Informe correspondiente al año 2018, obra citada.

292 Comisión Europea: Las nuevas normas sobre servicios de pago beneficiarán a los consumidores y a los minoristas. URL: http://europa.eu/rapid/press-release_IP-13-730_es.htm ◇ Consultado el 25 de febrero de 2019.

en la que se compra y paga, para lo cual introduce una serie de nuevos elementos a través de los cuales:

Se facilita y se hace más seguro el uso de los servicios, a través de la creación de nuevos servicios denominados de iniciación del pago, los cuales operan entre el comerciante y el banco del comprador y permiten pagos electrónicos baratos y eficaces sin recurrir al uso de una tarjeta de crédito.

Se prevén controles para estos nuevos servicios, al mismo tiempo que se dispone que los bancos y los demás proveedores de servicios de pago deberán intensificar la seguridad de las transacciones en línea.

Se protege a los consumidores contra el fraude, abusos e incidentes de pago.

Se aumentan los derechos de los consumidores en relación con la realización de transferencias, remesas y pagos.

Se promueve la aparición de nuevos operadores, así como el desarrollo de sistemas de pago móviles y a través de Internet.

La Directiva entró en vigencia en el año 2018, debiendo ser transpuesta a la legislación de los diferentes países. Como señala el bbva[293]: (I) Lleva cambios fundamentales en la industria al tener que dar acceso a terceros a la infraestructura de los bancos. (II) Promueve la competencia, beneficiando al consumidor en tanto nivela el terreno de juego entre países y entre proveedores de servicios de pago, abriendo la entrada a nuevos jugadores. (III) Establece estándares técnicos regulatorios, que son parte de la PSD2. (IV) Se han intensificado los requisitos de seguridad. (V) Los bancos deben abrir sus servicios de pago a terceras empresas (tpps), quienes deberán cumplir con las mismas reglas que los proveedores tradicionales, requiriendo: registro, autorización y supervisión de las autoridades. A modo de resumen, señalan que ahora el consumidor puede directamente autorizar a un comercio para que ejecute pagos en su nombre a través de su cuenta bancaria, utilizando una api (*Application Program Interface*), sin tener que recurrir a intermediarios.

Como puede verse, las Fintech han tenido un gran desarrollo en los últimos años, innovando y otorgando más soluciones, lo cual refleja el gran espacio que existía entre

293 BBVA: Todo lo que hay que saber de la PSD2. URL: https://www.bbva.com/es/lo-saber-la-psd2/ Consultado el 25 de febrero de 2019.

la oferta tradicional y las necesidades de las personas y de las empresas. La tecnología contribuye con la innovación y con el desarrollo, facilita la trasformación del sector tradicional; siendo fundamental el trabajo en conjunto y el diálogo entre los diversos actores del sector para conocer mejor las necesidades, las opciones existentes e innovar para poder cubrir de mejor forma los vacíos. Por otra parte, experimentar y revisar periódicamente las soluciones propuestas y los resultados obtenidos es esencial para poder realizar los ajustes que sean necesarios, en los tiempos debidos.

V. Economía digital

Como viene de indicarse, con el desarrollo de las plataformas, junto con la utilización de nuevas tecnologías, aplicándolo a diversos sectores, se ha desarrollado la economía digital, la cual permite ofrecer nuevos servicios, productos y soluciones sobre las redes de telecomunicaciones.

"*Cuando hablamos de ed (Economía Digital) nos referimos a aquellos productos y servicios virtuales, en todo o en parte, que son provistos a través de redes de comunicación. Su relevancia proviene de que prácticamente todos los sectores de actividad están atravesando –con diferentes velocidades– un proceso por el cual la parte "digital" del bien o servicio en cuestión es cada vez más relevante. Piense en la música, mapas, directorios de información o agencias de viaje. La combinación "digital + provistos en red" juega un rol fundamental en la conformación de la oferta, demanda y estrategias competitivas"*[294].

En la economía digital se ofrecen cada vez más servicios, productos y diversas soluciones en todo o en parte sobre las redes de telecomunicaciones, teniendo un impacto directo en toda la sociedad.

Como señala Luciana Macedo: *"La OCDE define la economía digital como compuesta por mercados basados en tecnologías digitales que facilitan el intercambio de bienes y servicios a través del comercio electrónico. La expansión del sector digital ha sido un motor clave del crecimiento económico en los últimos años, y el cambio hacia un mundo digital tiene efectos en la sociedad que se extienden más allá del contexto de la tecnología digital (OCDE, 2012). (...)*

294 SAROT, PABLO, "La Economía Digital" en *Revista de Negocios del IEEM,* abril 2016, Año 2019, N° 2, Montevideo.

Las características de los mercados digitales, en particular de las plataformas, promueven una mayor competencia en los mercados, ampliando su tamaño e intensificando la rivalidad. Pero, por otro lado, esas mismas características pueden llevar a una mayor concentración en los mercados y aún más, generar efectos anticompetitivos en los mercados.[295] ,,

Entre las características que se reconocen en la nueva economía se destaca[296]:

Que se trata de una economía de plataformas, con especial importancia en las capacidades complementarias. Por ejemplo: Internet es una plataforma, que tiene gran valor en otros sectores y permite a otras empresas brindar sus servicios. Lo mismo vemos con otros servicios digitales, como pueden ser las redes sociales o los servicios en las nubes.

Que las externalidades de red tienen gran influencia. A medida que más personas usan un determinado servicio, el mismo adquiere más valor. Lo anterior lo vemos mucho en las redes sociales, cuánta más personas haya en una determinada red, mayor valor adquiere, en tanto permite acceder a más personas, a su vez más personas van a querer ser parte, se puede llegar a más público, acceder a más información, vender más y mejor publicidad, ver tendencias, etc.

Que se tienden a crear mercados de un solo ganador, con posición dominante. Por ejemplo: Facebook, Google, Amazon, Apple, con la particularidad en este caso que además compiten entre ellos; por lo que se plantea que la mejor forma de competir es ofreciendo alguna capacidad específica.

Además presenta particularidades que la diferencian[297]:

1. Más innovación: la tecnología nos da la posibilidad de hacer pruebas rápidas, de forma económica, lo cual facilita que las empresas puedan innovar de forma más acelerada. Por ejemplo: a través de las Fintech, en su mayoría *startups*, se puede buscar atender diferentes líneas de negocios dentro de los servicios financieros,

---

[295] MACEDO, LUCIANA, "Economía digital y competencia" en *Estudios sobre los desafíos jurídicos ante la digitalización*, obra citada, pp. 257 y ss.

[296] Coursera: Digital Transformation. Dictado por Boston Consulting Group junto con University of Virginia, Darden School of Business.

297 ROGERS, DAVE de la Universidad de Columbia en curso *online* Coursera "Digital Transformation". Dictado por Boston Consulting Group junto con University of Virginia, Darden School of Business.

facilitando los servicios y ateniendo nichos, midiendo la respuesta y actuando en consecuencia.

2. Más competencia: la economía digital permite que cada vez haya nuevas empresas, por ende más competencia, en tanto borra fronteras entre sectores diferentes, y diversas empresas del mundo digital empiezan a tener presencia en nuevos mercados. Por ejemplo: uber repartiendo comida.

3. Más valor: la tecnología permite innovar en la forma en que prestamos el servicio o brindamos el producto. Por ejemplo: a través de las redes sociales podemos conocer más al cliente y crear más valor con pequeños cambios.

4. Más opciones de elegir: los clientes están más informados, tienen más opciones, lo cual les permite cambiar fácilmente de proveedor.

5. Más datos: gran cantidad de datos disponibles que pueden ser almacenados y procesados rápidamente, los cuales son aprovechables para las personas y para las empresas, quienes pueden utilizarlos para poder conocer mejor a los clientes, a los productos, enfocar en qué gusta más, qué menos y hacer los ajustes que sean necesarios para mejorar los productos y/o servicios. Por ejemplo: Netflix en base a los datos que tiene de nosotros, el tipo de película o serie que solemos ver, nos hace sugerencias en línea con nuestro perfil.

Hay diversas formas en que las empresas pueden usar los datos, incluso los usan para prestar servicios a otras. A modo de ejemplo[298]:

Hay empresas que reúnen datos de gran variedad de fuentes –como puede ser el registro electoral, los fallos judiciales, etc.–, elaboran un perfil en base a dicha información y califican el riesgo de otorgar determinados préstamos. por ejemplo: experian actúa como una empresa de puntuación de crédito.

Otras empresas recopilan datos de sus clientes de diversas fuentes –por ejemplo a través de las tarjetas de fidelización, del análisis de las compras, de cuando interactúan en el sitio web de la empresa, etc.– para poder conocer los hábitos de compra y así mejorar sus servicios y productos. De esta manera pueden generar ofertas o promociones especiales que se adapten a las necesidades y gustos de sus consumidores,

298 MURRAY, ANDREW, *Information technology law,* Oxford University Press, Oxford, 2016, pp. 542 y ss.

puede identificar tendencias, así como reaccionar rápidamente para que la oferta responda a la demanda. Se suele decir que es el método que utiliza el grupo Inditex.

También hay empresas que se dedican a investigar mercados para lo cual necesitan datos, que recopilan de diversas fuentes, que les permiten elaborar perfiles y vender sus conocimientos a otras empresas. Hay estudios de mercados tradicionales y también los hay a través de compañías de Internet. El ejemplo más conocido es el de Google, quien a través de su buscador recopila gran cantidad de datos y luego vende publicidad especializada en línea enfocada en el público objetivo.

Asimismo, hay compañías que recopilan información –por ejemplo de los hábitos en Internet– como intermediarios de otras y venden los datos como paquetes que ayudan a desarrollar productos, así como para enfocar la publicidad. El ejemplo más conocido son las redes sociales, como por ejemplo Facebook.

Por último, hay empresas que generan grandes bases de datos, que luego son utilizadas para enviar correos o llamadas para intentar vender sus productos y/o servicios.

Con la digitalización de la información y todos los datos que hay en línea, se han desarrollado diversos programas y tecnologías que nos permiten almacenar, procesar y analizar toda la información a gran velocidad, de manera simple, económica y automatizada, pudiendo ver, predecir y tomar decisiones más informadas en tiempo real.

Sin duda lo anterior tiene muchos beneficios, pero también implica muchos riesgos. Hay temas de seguridad, de privacidad, de categorizar los datos –las computadoras no tienen, por lo menos aún no la mayoría, la habilidad para determinar la naturaleza o la sensibilidad de la información–, debiendo buscar la mejor forma de proteger los derechos fundamentales de las personas, sobre todo su intimidad.

Un caso muy conocido se dio a conocer hace unos años por el New York Times, cuando el padre de una adolescente fue a quejarse con una empresa en tanto le estaban enviando a su hija cupones de descuentos para cosas de bebés, lo cual teóricamente no tenía sentido. La empresa se disculpó con el padre al verificar que efectivamente se le estaban haciendo esos envíos a su hija. Posteriormente, el padre confirmó que la

adolescente estaba embarazada, lo cual explicaba por qué la empresa le estaba haciendo ese tipo de comunicaciones[299].

Como muchas otras organizaciones, según se difundió[300], dicha empresa recopilaba datos de sus clientes de múltiples fuentes. Por ejemplo: de todo lo que los clientes compran en la tienda, si usan tarjeta de crédito, un cupón de descuento, si completa una encuesta, de cuando llaman al servicio al cliente, cuando abren un correo que envía la empresa, cuando visitan su sitio web; pero van más allá, y también se recolecta información sobre la edad, sobre el estado civil, si tiene hijos, en dónde vive, el tipo de artículo que lee, los temas que habla online, las búsquedas que realiza en la web, entre otros múltiples ejemplos, todo lo cual permite elaborar perfiles y segmentar.

Incluso hay diversas fuentes que, de igual forma, permiten acceder a más información como ser la historia laboral, el tipo de revistas que se lee, si alquila o compró propiedad, qué tipo de temas se hablan más online, a qué páginas se ingresan más y por cuánto tiempo se está, entre otros múltiples ejemplo[301].

La mayoría de estos datos, por sí solos nos dicen poco, pero si se analizan, enlazan, almacenan y procesan adecuada y coherentemente, se pueden elaborar perfiles, segmentar, conocer tendencias, así como sacar conclusiones de mucho valor, actuando sobre las mismas[302].

En esta mismo sentido, y a modo de antecedente, es interesante comentar cómo comenzó Amazon a experimentar con estas herramientas. El planteo inicial fue qué pasaría si la compañía pudiera recomendar libros específicos a los clientes en base a sus preferencias de compra. Disponían de gran cantidad de datos sobre sus clientes, a modo de ejemplo: qué compraban, qué libros veían pero no compraban, etc., la cual procesaron de forma tradicional, analizándola para encontrar similitudes entre los clientes. Si bien daban muchos resultados, las recomendaciones que surgían no eran muy buenas, en tanto una persona compraba un libro de Polonia y ya se la inundaba con publicidad sobre comida en Europa del Este. En vista de que los resultados no eran muy

299 Nota de prensa: https://www.nytimes.com/2012/02/19/magazine/shopping-habits.html Consultado el 20 de febrero de 2019.

300 Forbes, URL: https://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/?sh=d47843866686 Consultado el 20 de febrero de 2019.

301 ARAMENDIA, MERCEDES, "La privacidad y las TIC", en *Estudios de Información Pública y Datos Personales*, Tomo III, Universidad de Montevideo, 2018, pp. 179 y ss.

302 Ibidem.

exactos, revieron la forma de analizar y comparar la información, y se dieron cuenta de que no era necesario comparar a las personas con otras, sino que necesitaban encontrar asociaciones entre los propios productos, lo cual les generó una gran diferencia, la cual se potenció aún más cuando se diversificó para comercializar otros productos, además de libros.[303]

No hay dudas de que la información a la que se accede al procesar los datos, utilizando diversas tecnologías como big data, ofrece muchos beneficios para todas las empresas y organizaciones, en tanto les permiten poder tomar decisiones informadas a mayor velocidad, evitando errores y pudiendo predecir tendencias. Muchos actores y sectores se favorecieron con estos cambios, se suele destacar al sector del marketing, especialmente a quienes se dedican a la publicidad, pero también al sector financiero, al de seguros y a las administraciones públicas; sin perjuicio de que las empresas del sector de la tecnología y de la información han sido las pioneras en utilizar y beneficiarse del Big Data, mejorando su productividad y sus servicios[304]. Otro sector que también se destaca por los beneficios es el de la salud pública, pero en general todos los sectores de servicios, siendo un buen ejemplo el de comprar tickets de avión[305].

El uso de estas tecnologías es realmente maravilloso, combinando miles de millones de datos, compañías pueden identificar la prevalencia de la gripe casi tan bien como los datos oficiales, más rápido, así como predecir la volatilidad del precio de un boleto de avión. Lo anterior solo es una muestra del gran valor que puede generar los datos y que sacude todo: *¨desde los negocios y las ciencias hasta la salud, el gobierno, la educación, la economía, las humanidades y todos los demás aspectos de la sociedad"*[306].

---

[303] MAYER-SCHÖNBERGER, VIKTOR Y CUKIER, KENNETH, ¨ Big Data - A Revolution that will transform how we live, work and think¨, MURRAY, JOHN, Gran Bretain. 2013, pp. 50 y ss.

[304] PUYOL MONTERO, JAVIER, en obra citada, pp. 77.

[305] *¨Public Health in only one area where big data is making big difference. Entire business sectors are being reshaped by big data as well. Buying airplane tickets is a good example¨* MAYER-SCHÖNBERGER, VIKTOR y CUKIER, KENNETH, ¨ Big Data - A Revolution that will transform how we live, work and think¨, MURRAY, JOHN, Gran Britain, 2013, pp. 3.

[306] MAYER-SCHÖNBERGER, VIKTOR y CUKIER, KENNETH, en obra citada, pp. 11. *¨With information, as with physics, size matter. Hence, Google is able to identify the prevalence of the flu just about as well as official data based on actual patient visits to the doctor. It can do this by combing through hundreds of billions of search terms –and it can produce an answer in near real time, far faster than official sources. Likewise, Etzioni´s Forecast can predict the Price volatility of an airplane ticket and thus shift substantial economic power into the hands of consumers. But both can do so well only by analyzing hundreds of billions of data point.*

Sin duda, todas estas posibilidades tiene múltiples beneficios, mas genera inquietudes respecto a la privacidad, en tanto –por ejemplo- al tratar de forma automatizada cientos de datos, muchas veces se procesan datos personales –incluso sensibles- sin siquiera advertirlo. Además, la realidad es que *¨mediante la utilización de las técnicas informáticas y de la transmisión de datos entre ordenadores, con su capacidad de proceso, se puede ejercer un control social y, sin que la persona llegue a percatarse, interferir en su vida¨*[307].

Ante este tipo de planteos hay quienes suelen plantear si cuando buscamos en Internet – como puede ser el buscador de Google- o cuando consultamos a los asistentes personales –como puede ser Alexa- sobre determinados aspectos, como podría ser dónde comprar determinado producto o contratar determinado servicio, si nos están respondiendo de forma transparente, ética, o si en realidad de cierta forma se nos manipula en función de la publicidad que se les abona.

Al respecto, resulta realmente interesante lo comentado por Mayer-Schönberger Viktor y Cukier Kenneth, quienes señalan que durante casi cuarenta años, hasta que se derrumbó el Muro de Berlín en 1989, se espiaba a millones de personas, se observaba y analizaba todo: calles, autos, cartas, cuentas bancarias, apartamentos, líneas telefónicas; llevando además a que las propias personas se espiaran entre sí, afectando la confianza de todos, incluso en los círculos más íntimos, como podría ser la relación entre las familias. Actualmente, muchos años después de que desapareció esa realidad, nos enfrentamos a que se están recopilando y almacenando muchos más datos de los que se incautaban incluso en ese momento, y no solo se hace para vigilancia pública, buscando la seguridad pública, sino para poder conocer nuestros hábitos de compra, de búsqueda, cómo pensamos, con quién hablamos, hasta para saber a quién tenemos cerca.[308]

These two examples show the scientific and societal importance of big data as well as the degree to which big data can become a source of economic value. They mark two ways in which the world of big data is poised to shake up everything from business and the sciences to healthcare, government, education, economics, the humanities, and every other aspect of society¨

[307] DAVARA, MIGUEL, ¨Manual de Derecho Informático¨, 6ta Edición, Ed. Aranzadi, Cizur Menor, Navarra, 2004, pp 43.

[308] MAYER-SCHÖNBERGER, VIKTOR y CUKIER, KENNETH, obra citada, pp. 150 y 151. Traducción propia del siguiente texto: "*For almost forty years, until the Berlin Wall came down in 1989, the East German state secutiry agency known as the Stati spied on millions of people. Employing around a hundred thousand full-time staff, the Stati watched from cars and streets. It opened letters and peeked into bank accounts, bugged apartments and wiretapped phone lines. And it induced lovers and couples, parents and children, to spy on each other, betraying the*

Ante toda esta realidad, la privacidad, la confianza y la transparencia toman cada vez mayor importancia, teniendo preeminencia empoderar a las personas, para que puedan controlar sus datos, su información, que puedan conocer qué datos se recopilan, por qué, para qué y que se almacenen otorgando la seguridad necesaria para evitar un mal uso de los mismos.

Por otra parte, los temas de seguridad cada vez se plantean con mayor énfasis, sobre todo por los robos de información que se han difundido en los últimos tiempos y por los daños que esto puede generar tanto para las personas, cuyos datos están directa o indirectamente involucrados, como para las organizaciones que sufren el quiebre, viendo en muchos casos dañada su reputación, su confianza, así como su valor.

Las consecuencias pueden ser realmente muy graves, habiéndose difundido diversos casos en que las personas afectadas por el robo de los datos, han llegado a cometer suicidio, además de ser objeto de extorsiones[309].

Las empresas deben proteger los datos de sus clientes, no solo por los daños que les pueden llegar a generar ante un ciberataque, sino que también es un factor cada vez más importante que los usuarios e inversionistas confíen en sus servicios y los elijan.

Al respecto, como señala Ryan Polk, Policy Advisor de Internet Society[310], al comentar el robo de datos que sufrieron los registros de más de 500 huéspedes de la división Starwood del Hotel Marriot International en el año 2018; si bien la información

---

most basic trust humans have in each other. The resulting files –including at leat 39 million indez cards and 70 miles of documents- recorded and detailed the most intimate aspects of the lives of ordinary people. East Germany was one of the most comprehensive surveillance states ever seen.
Twenty years after East Germany´s demise, more data is being collected and stored about each one of us than ever before. We´re under constant surveillance: when we use our credit cards to pay, our cell phones to communicate, or our Social Security numbers to identify ourselves. (…) The Internet has made tracking easier, cheaper, and more useful. And clandestine three-letter government agencies are not the only ones spying on us. Amazon monitors our shopping preferences and Google our browsing habits, while Twitter knows what´s on our minds. Facebook seems to catch all that information too, along with our social relationships. Mobile operator Know not only whom we talk to, but who is nearby.".

[309] "Chantajes, amenazas y suicidios, consecuencias del robo de datos de Ashey Madison" URL: https://www.20minutos.es/noticia/2540918/0/ashley-madison/chantajes-amenazas/consecuencias-robo-datos-usuarios / Consultado el 20 de julio de 2019. Los casos ocurrieron en Canadá tras filtrarse información de una plataforma que se dedicaba a generar aventuras para personas casadas.

[310] Internet Society, Ryan Polk, URL: https://www.internetsociety.org/es/blog/2018/12/los-datos-de-clientes-no-siempre-son-un-activo-lecciones-del-robo-de-datos-de-marriott/ Consultado el 30 de enero de 2019.

es un activo -siendo en este caso uno de los principales argumentos utilizados en el año 2016 por Marriot International al adquirir Starwood, específicamente por los programas de fidelidad y los datos de sus clientes-, también conlleva responsabilidad -en tanto, por ejemplo: no se ha podido confirmar si solo se ha llegado a datos personales como nombre, correo, teléfono, o si también han accedido a números de tarjeta de crédito u otro tipo de información-. Este incidente, en pocas horas ocasionó que las acciones de Marriot cayeran más del 5%, además de afectar la confianza de los clientes, lo cual implica recursos y costos; al tiempo que muestra que cada vez es más importante la seguridad digital y el tratamiento que se hace de los datos -pareciera que quienes irrumpieron los datos ya los habían hecho anteriormente-.

Todos estos fenómenos están ocurriendo globalmente, generando que múltiples y diversos actores estén trabajando sobre la temática, planteando la necesidad de fijar principios y bases de actuación que pongan en el centro los derechos fundamentales de las personas. Se debe respetar la dignidad de las personas, se les tiene que dar seguridad, al tiempo que se tiene que trabajar en conjunto entre los diversos actores de la sociedad -gobiernos, empresas, ciudadanos, sociedad civil, academia, así como todos quienes tengan interés en la temática y quieran aportar-, a fin de generar conciencia y educación.

Vale comentar que muchas empresas y organizaciones están viendo justamente en estos riesgos la posibilidad de diferenciarse.

A modo de ejemplo, en el Foro Económico Mundial de Davos de 2019, la GSMA presentó la ¨Declaración Digital¨. Según manifiestan en su página web, *¨la declaración establece pautas fundamentales para actuar de forma ética en la era digital, ayudando a las empresas a brindar a los ciudadanos, la industria y los gobiernos lo que más les importa. Los 40 líderes empresariales que ya se han comprometido con la declaración abarcan varios sectores de la industria e incluyen representantes de: Bharti Airtel, China Mobile, China Telecom, Deutsche Telekom, Ericsson, IBM, KDDI, KT, LG Electronics, Mobile World Capital Barcelona, Nokia, NTT DOCOMO, Orange, Samsung Electronics, Sharp, SK Telecom, Sony Corporation, STC Group, Telefónica, Turkcell, Verizon, Vodafone y Xiaomi.*

La iniciativa surge en contexto de los enormes cambios sin precedentes que afectan a las empresas y consumidores en el mundo digital. Se espera que para 2022, el 60 por ciento del PBI se digitalice.1 La llegada inminente de las redes 5G acelerará todavía más este cambio. Al mismo tiempo, los consumidores exigen –con razón- cada

vez más prestaciones de los servicios digitales, al tiempo que ponen a prueba su confianza en las empresas."[311]

En esta misma línea, según ha trascendido en prensa, "*Tim Cook, máximo directivo de Apple, ha insistido en que la Federal Trade Commission (FTC, Comisión Federal de Comercio, el organismo regulador estadounidense) otorgue a los usuarios un mayor control sobre la información que se recopila acerca de ellos y ha cargado contra la proliferación de lo que ha llamado una economía secreta e incontrolada de compraventa de datos.*

Cook exhorta al Congreso a aprobar "una legislación federal integral sobre la privacidad", con provisiones que exijan que las firmas minimicen la recolección de datos sobre los consumidores y faciliten a estos el "acceso, corrección y eliminación" de los datos acumulados.

También afirma que la FTC podría implantar nuevas protecciones mediante la creación de un "centro de coordinación de los revendedores de datos" en el que estos deberían inscribirse. Así los usuarios podrían estar al corriente de las ventas que incluyan información sobre ellos y darles un mayor poder para, en palabras de Cook, "borrar sus datos a petición, de una vez por todas, mediante un procedimiento gratuito, fácil y en línea".

"Los consumidores no tienen por qué tolerar que las empresas sigan elaborando sin responsabilidad alguna perfiles detallados de los usuarios, que se produzcan filtraciones de datos que parecen escapar a todo control y que el control sobre nuestra propia vida digital sea cada vez más tenue." (...)

En el congreso WWDC para desarrolladores que la firma celebró en junio de 2018, Apple atacó a Facebook y a Google por sus prácticas de recolección de datos e implantó nuevas funcionalidades en iOS para impedir la obtención de datos sobre el usuario y sus actividades. Apple ha vuelto a marcar su posición sobre la privacidad en el CES con un gigantesco cartel que destacaba sobre el recinto ferial y decía: "What

[311] GSMA, URL https://www.gsma.com/newsroom/wp-content/uploads//2019_01_24-Digital-Declaration_press-release_GSMA_FINAL-under-embargo-SPA_FINAL2.pdf Consultado el 30 de enero de 2019.

happens on your iPhone, stays on your iPhone" ("Lo que sucede en tu iPhone, se queda en tu iPhone.")[312]".

En este mismo sentido se ha expresado Tim Berners-Lee, considerado el padre de Internet, quien inventó en los años 80 la "world wide web" (www), destacando la necesidad de que los usuarios de la red vuelvan a tener el control de sus datos[313], para lo cual ha desarrollado una nueva plataforma llamada Solid.

Considerando lo anterior, no hay dudas de que la información se puede utilizar para fines muy buenos y generar mucho valor, pero también tiene muchos riesgos para la intimidad y la seguridad. Hay que asegurar los derechos fundamentales de las personas, que las mismas conozcan qué datos se recopilan, por qué, para qué y que se almacenen otorgando la seguridad necesaria para evitar un mal uso de los mismos.

No cabe duda de la actualidad de la temática y los múltiples desafíos que plantea para todos, generándose nuevas reglamentaciones, innovadoras, que buscan de diversas maneras devolver el control de los datos a las personas y proteger su privacidad.

En esta línea y considerando lo establecido en el Reglamento General de Protección de Datos (rgpd o gdpr) de la ue, se suele indicar la importancia de establecer estándares que garanticen la seguridad de los datos, así como que los mismos sean los necesarios para el fin, estén actualizados y que las personas puedan ejercer sus derechos: acceso, rectificación, cancelación, oposición. Asimismo, el derecho al olvido y el de la portabilidad de los datos.

Al respecto, el rgpd dispone que *"Los interesados deben tener derecho a acceder a los datos personales recogidos que le conciernan y a ejercer dicho derecho con facilidad y a intervalos razonables, con el fin de conocer y verificar la licitud del tratamiento. (...) Todo interesado debe, por tanto, tener el derecho a conocer y a que se le comuniquen, en particular, los fines para los que se tratan los datos personales, su plazo de tratamiento, sus destinatarios, la lógica implícita en todo tratamiento automático de datos personales y, por lo menos cuando se base en la elaboración de perfiles, las consecuencias de dicho tratamiento".*

---

[312] "Tim Cook ataca la compraventa de datos" en TyN Magazine. URL: https://www.tynmagazine.com/tim-cook-ataca-la-compraventa-de-datos/ . Consultado el 30 de enero de 2019.

[313] https://www.trecebits.com/2018/10/02/tim-berners-el-inventor-de-la-web-quiere-revolucionar-internet/ consultado el 30 de enero de 2019.

Asimismo señala que, *"A fin de garantizar un tratamiento leal y transparente respecto del interesado, (...) responsable del tratamiento debe utilizar procedimientos matemáticos o estadísticos adecuados para la elaboración de perfiles, (...) de forma que se tengan en cuenta los posibles riesgos para los intereses y derechos del interesado y se impidan, entre otras cosas, efectos discriminatorios en las personas físicas por motivos de raza u origen* étnico*, opiniones políticas, religión o creencias, afiliación sindical, condición genética o estado de salud u orientación sexual, o que den lugar a medidas que produzcan tal efecto. Las decisiones automatizadas y la elaboración de perfiles sobre la base de categorías particulares de datos personales* únicamente *deben permitirse en condiciones específicas."*

Como se ve, se presta especial atención al uso que se hace de los datos y al tratamiento que se hace de los mismos. Se pueden automatizar los datos y utilizar para buenos fines, pero hay que tomar las previsiones necesarias para no afectar los derechos fundamentales de las personas.

Es interesante señalar que el Estado de California, uno de los líderes mundiales en el desarrollo de nuevas tecnologías, aprobó en junio de 2018, que entrará en vigencia a partir del 1º de enero de 2020, *¨La Ley de Privacidad del Consumidor de California de 2018¨*[314].

Parte de la base de que la Constitución de California incluye el derecho a la privacidad como un derecho inalienable de todas las personas, para el cual es fundamental que los individuos puedan controlar el uso, incluida la venta, de su información personal.

Reconoce que actualmente es prácticamente imposible solicitar trabajo, criar niños, conducir un automóvil o hacer un cita sin compartir información personal. Al mismo tiempo, destaca que el rol de las tecnología en la vida diaria crece constantemente, habiendo por ende un aumento en la cantidad de información personal que se comparte por los consumidores con las empresas. A modo de ejemplo, señala que las empresas saben dónde viven los consumidores, la cantidad de hijos que tienen, qué tan rápido conducen, la personalidad del individuo, los hábitos de dormir,

[314] https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375 Consultado el 30 de enero de 2019.

información biométrica y de salud, información financiera, las redes sociales, solo por mencionar algunos casos.

Considera que la regulación actual no siguió el ritmo de estos desarrollos, ni las implicaciones que tiene para la vida la recopilación, el uso y la protección de la información personal. Reconoce que las personas desean privacidad y más control sobre su información, por lo que adopta mecanismos para salvaguardar su privacidad, incluida la privacidad en línea y la de los menores, para que las personas sepan quién, qué, dónde, cuándo y cómo las empresas manejan la información personal que recogen.

En esta línea busca asegurar los siguientes derechos: (i) que puedan saber qué información personal de ellos se está recolectando; (ii) que puedan conocer si su información personal es vendida o revelada y a quién; (iii) que puedan oponerse a la venta de su información personal; (iv) que puedan acceder a su información personal; (v) que no sean discriminados por ejercer los derechos que la ley les otorga.

Busca que los consumidores tengan el derecho de solicitar a empresas que les revelen la información personal que recopilan, las fuentes y los fines para los que la recolectan – si es para usos comerciales propios o para venderla o compartirla con terceros-. Además se le otorga el derecho a los consumidores a solicitar que se elimine su información personal, así como a oponerse a que se vendan sus datos, prohibiendo a las empresas discriminar a los consumidores que ejerzan ese derecho. No obstante, se autoriza a las empresas a ofrecer incentivos financieros para la recopilación de información personal.

Asimismo, se define información personal haciendo referencia a diferentes características, comportamientos personales y comerciales, así como diversas inferencias que se extraen de la información.

En definitiva, toda esta nueva realidad, más allá de los riesgos que conlleva, ha generado múltiples beneficios para la economía y para la sociedad digital, en tanto se traduce en más eficacia, al tiempo que facilita la innovación basada en los datos, borra fronteras y le da a los consumidores más posibilidades de elegir, reforzando el bienestar de las personas y la competitividad.[315]

315 Comunicado de la Comisión UE, obra citada.

Por otra parte, nadie duda de que gracias al alcance y a las facilidades que las plataformas digitales tienen, se ha intensificado la participación de los ciudadanos en la sociedad y en la democracia, promoviendo la libertad de expresión, así como facilitando compartir y acceder a la información. Sin perjuicio, también conlleva múltiples riesgos, como puede ser: la difusión de noticias falsas, la manipulación de los datos para fines espurios o poco éticos, generar daños a la propiedad intelectual, entre otros ejemplos.

En suma, junto con los beneficios, se presentan desafíos, que necesariamente se deben identificar y sobre los cuales hay que trabajar. En primer lugar, para que las personas y las empresas sean parte del mundo digital y confíen en él, se identifica la necesidad de garantizar la competencia, la protección de los consumidores, la protección de los datos personales y la libertad de elegir. En segundo lugar, dada la naturaleza transfronteriza de las plataformas digitales, es importante la cooperación entre las diversas autoridades competentes, así como el trabajo y la coordinación a nivel regional e internacional. En tercer lugar, la innovación ha sido la clave del gran desarrollo que se ha producido y es esencial que se siga promoviendo, por lo que a la hora de regular puede ser favorable atender los problemas específicos que se vayan planteando, analizar si el marco normativo actual sigue siendo adecuado o si debe ser ajustado. El diálogo constante entre los diversos actores del sector es primordial, así como el modelo de trabajo *multistakeholders*, complementado por la autorregulación y los principios[316].

En esta línea, es interesante comentar sobre los principios tomados por la Comisión Europea, en tanto parecen muy adecuados[317]:

1. Aplicar las mismas condiciones para servicios digitales comparables a fin de garantizar una competencia leal: los nuevos modelos prestados sobre las plataformas, compiten con los servicios tradicionales, incentivándolos a innovar y a mejorar. Desafían los modelos tradicionales, los sustituyen en muchas ocasiones, mas no siempre están sometidos a las mismas reglas. Se plantea la necesidad de simplificar, modernizar y aligerar la reglamentación existente, y que se evite poner cargas desproporcionadas.

2. Exigir conducta responsable para proteger los valores fundamentales: se reconoce el rol cada vez más importante que tienen las plataformas para el acceso a la

316 Ibídem.
317 Ibídem.

información y a los contenidos. Se quiere en general una mayor transparencia en la política de las plataformas, se destaca que hay mucho contenido perjudicial para menores o que siembran el odio, al tiempo que se utilizan contenidos de terceros sin los debidos permisos. Considerando lo anterior, a fin de garantizar los derechos fundamentales, se ve como necesario revisar la regulación de los servicios de comunicación audiovisual, mantener el régimen de responsabilidad de los intermediarios, atendiendo el enfoque sectorial para resolver problemas, proteger los derechos de autores, así como buscar la forma de incrementar la autorregulación coordinada.

3. Necesidad de transparencia y equidad para mantener la confianza de los usuarios y salvaguardar la innovación: se debe informar y empoderar a los ciudadanos y a los consumidores. El acceso a los datos contribuye con la eficiencia del mercado y de la innovación, mejora la educación, los trabajos y los servicios del Estado. Pero no se va a poder desarrollar con éxito, sin la confianza de los usuarios en las plataformas en línea y si no se respetan sus derechos e intereses. Al respecto, toma mayor importancia el consentimiento explícito y la introducción de la protección de los datos por defecto y desde el diseño. Por otra parte, es importante que las plataformas sean transparentes, no induzcan a error a los consumidores, como puede ser el recomendar en las búsquedas resultados patrocinados.

Asimismo, considerando el rol y la importancia que tienen las plataformas en la economía, para la prestación de otros bienes y servicios, así como para acceder a información, las condiciones de acceso tienen cada vez mayor relevancia, sobre todo en lo que respecta a la realización de prácticas comerciales desleales, como pueden ser: (i) que nieguen el acceso o que modifiquen unilateralmente las condiciones; (ii) que en ocasiones desempeñan un doble papel, en tanto facilitan el acceso al mercado y compiten en el mismo con otros proveedores, lo que plantea el riesgo de que promuevan indebidamente sus propios servicios en detrimentos de los otros; (iii) que incorporen cláusulas abusivas que perjudiquen al consumidor; (iv) que no haya transparencia en la utilización de los datos, en los resultados de búsqueda, lo cual pueda dañar las actividades comerciales de otras empresas. Como ejemplo de lo anterior, se señala que en junio de 2017 se adoptó una decisión en la que concluía que Google había abusado de su posición dominante, al otorgar una ventaja ilícita a su propio servicio de comparación de precios en sus resultados de búsqueda generales.

Considerando esta situación, en abril de 2018 la Comisión Europea presentó una propuesta de regulación a fin de establecer normas sobre transparencia y equidad para proporcionar más seguridad a las empresas y comerciantes más pequeños cuando utilicen las plataformas en línea. Asimismo, se creó un observatorio de la UE a efectos de supervisar los efectos de la normativa y su evolución[318].

4. Garantizar mercados abiertos y no discriminatorios basados en la economía de datos: se hace énfasis en la importancia de que los usuarios puedan cambiar fácilmente de proveedor. Asimismo, que el usuario pueda tener la libertad de conservar una determinada plataforma, de compartir sus datos y que no se le establezcan obstáculos. Sobre este punto, se plantea a la portabilidad y la interoperabilidad como posibles soluciones para la libre circulación de datos, así como para facilitar a las empresas y a los usuarios el cambio entre diferentes plataformas en línea y servicios de computación en la nube.

En esta línea, el 28 de febrero de 2018 se aprobó el Reglamento (UE) 2018/302 del Parlamento Europeo y del Consejo, sobre medidas destinadas a impedir el bloqueo geográfico injustificado y otras formas de discriminación por razón de la nacionalidad, del lugar de residencia o del lugar de establecimiento de los clientes en el mercado interior y por el que se modifican los Reglamentos (CE) Nº 2006/2004 y (UE) 2017/2394 y la Directiva 2009/22/CE[319]. El Reglamento no se aplica a situaciones que se limitan al interior de un único Estado, a los servicios financieros (establecidos en el artículo 2, apartado 2, de la Directiva 2006/123/CE) y no afectará Directiva 2001/29/CE del Parlamento Europeo y del Consejo).

Define "Servicios prestados por vía electrónica" a aquellos *"servicios prestados a través de internet o de una red electrónica que, por su naturaleza, se presten de manera básicamente automatizada y con una intervención humana mínima, y sin que se puedan*

318 Comisión Europea, Comunicado de Prensa: "Plataformas en línea: la Comisión establece nuevas normas sobre transparencia y equidad". URL: https://ec.europa.eu/digital-single-market/en/news/regulation-promoting-fairness-and-transparency-business-users-online-intermediation-services Consultado el 20 de febrero de 2019.

319 Reglamento (UE) 2018/302 del Parlamento Europeo y del Consejo, de 28 de febrero de 2018, sobre medidas destinadas a impedir el bloqueo geográfico injustificado y otras formas de discriminación por razón de la nacionalidad, del lugar de residencia o del lugar de establecimiento de los clientes en el mercado interior y por el que se modifican los Reglamentos (CE) n.° 2006/2004 y (UE) 2017/2394 y la Directiva 2009/22/CE (Texto pertinente a efectos del EEE.), https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32018R0302 Consultado el 13 de julio de 2019.

garantizar a falta de tecnología de la información[320]*"* e "interfaz en línea" como "*cualquier tipo de programa informático, incluidos los sitios web o parte de ellos y las aplicaciones, incluidas las aplicaciones móviles, utilizado por un comerciante o en nombre de este, que sirva para dar a los clientes acceso a los productos o servicios del comerciante con vistas a iniciar una operación con respecto a dichos productos o servicios*[321]"

Interesa destacar que se prohíbe por motivos relacionados con la nacionalidad, el lugar de residencia o con el lugar de establecimiento del cliente: (i) bloquear o limitar el acceso de los clientes a las interfaces en línea; (ii) redirigir a ese cliente a una versión de su interfaz que sea diferente y específica para dichos clientes, salvo que el cliente del consentimiento expreso para ello; (iii) aplicar condiciones generales de acceso diferentes a los productos y servicios; (iv) aplicar condiciones de pago distintas cuando se efectúa la transacción de forma electrónica, mediante transferencia, adeudo domiciliado u otro instrumento de pago, cuando se cumplan con la Directiva (UE) 2015/2366, y la operación se efectúe en una moneda que el comerciante acepte.

Vale destacar que para poder ejecutar este Reglamento cada Estado miembro debe designar uno o varios organismos responsables, además debe proporcionar asistencia práctica a los consumidores en caso de litigio entre un consumidor y un comerciante, y cada cinco años la Comisión debe presentar un informe evaluando el impacto del Reglamento en el mercado interior y el comercio electrónico transfronterizo.

Sin duda, todo este nuevo contexto, presenta múltiples retos que requiere analizar la situación actual y hacer cambios a fin de poder responder de la mejor manera ante las nuevas necesidades.

En algunos casos los nuevos servicios y aplicaciones aparecen como soluciones completamente nuevos, disruptivas; mas en otros casos, simplemente innovan en la forma o en el medio en que prestan el servicio o comercializan los productos, compitiendo directamente con los servicios tradicionales y escapando, en algunos casos, de la regulación y de las cargas.

Las empresas digitales han tenido un gran auge y las empresas tradicionales están teniendo que transformarse para poder competir. Lo anterior plantea el dilema de que

[320] Artículo 2.1) del Reglamento (UE) 2018/302.
[321] Artículo 2.16) del Reglamento (UE) 2018/302.

mucha de la normativa actual, como ser la normativa fiscal, no tuvo en cuenta esta nueva realidad, en la que las empresas operan de forma virtual, sin presencia física o con muy poca, generando en algunos casos competencia desleal.

Como informó la Comisión Nacional de los Mercados y de la Competencia (cnmc) de España[322] *"Los servicios ott (del inglés "over the top") han crecido en número y en usuarios a medida que aumentaba la penetración de la banda ancha y la velocidad de conexión de la misma." (...) "...no hay una definición unánime de lo que constituye un servicio ott, cabe considerar que mucho de lo que se consume y distribuye en Internet es un servicio ott. Así, los juegos* online, *las redes sociales, los contenidos audiovisuales, las distintas aplicaciones y gran parte del comercio electrónico son servicios ott. Estos servicios se pueden categorizar atendiendo a distintas dimensiones. Por ejemplo, existen servicios de negocio y servicios ofertados sin ánimo de lucro. Entre los primeros, hay diversas formas de generar ingresos: pagos por consumos y/o por subscripción, ingresos por publicidad e incluso ingresos derivados de la venta de información sobre los patrones de comportamiento y características de sus usuarios. En Internet conviven servicios enteramente producidos por profesionales, con aquellos cuyo éxito depende de las contribuciones de los usuarios finales, que distribuyen o comparten contenidos sobre soportes de terceros".*

Como surge en el "*Manifiesto Digital. Por una Internet, abierta y segura para todos*"[323] de Telefónica, *"La economía digital ha cambiado la dinámica competitiva de muchos mercados, haciendo que muchas normas y reglamentos queden obsoletos o dejen de ser necesarios. Además, una normativa inadecuada puede obstaculizar la innovación y el nacimiento en el mercado de nuevos modelos comerciales y atractivos servicios digitales. Urge, por tanto, encontrar una estrategia más inteligente y eficaz. En muchos casos no es necesario ningún tipo de regulación adicional. Los responsables políticos deberían realizar un análisis minucioso y con proyección de futuro que permita definir los resultados deseados de las políticas, y así redactar una normativa adecuada, eliminando las ya obsoletas."*[324]

322 https://www.cnmc.es/sites/default/files/1533234_0.pdf Consultado el 5 de octubre de 2017.

323 https://www.telefonica.com/documents/341171/362460/Manifiesto_Digital/e0652543-fbed-45c5-ba9c-74e16c08a69d Consultado el 20 de febrero de 2019.

324 STECK, CHRISTOPH, "Manifiesto Digital. Por una Internet abierta y segura para todos", Telefónica, S.A. pág. 104. https://www.fundaciontelefonica.com/cultura-

Para esta revisión, en el Manifiesto Digital se proponen tres principios: convergencia de los mercados, reglas de juego uniformes y un entorno propicio para la inversión. En relación a la convergencia, destaca que actualmente se compite con entidades y servicios que anteriormente operaban en mercados distintos. Respecto a reglas de juego uniformes, señala la importancia de que los mismos servicios se rijan por las mismas normas, independientemente de las tecnologías que utilicen para ser prestados. Finalmente en relación al entorno propicio para la inversión, subraya que este nuevo mundo tiene una gran necesidad de conectividad para que todos tengan acceso a Internet y a los nuevos servicios, y para que este desarrollo sea posible es fundamental que se realicen grandes inversiones, desplegando redes e infraestructura.

Lo anterior no significa que haya que regular los nuevos servicios, sino que habría que analizar las normativas vigentes y ajustar todo lo que sea necesario, planteando si es preciso una regulación ex ante –como se ha hecho en muchos casos hasta ahora– o si es más efectivo, facilitando la innovación y el desarrollo, una política por sector de actividad y de defensa de la competencia caso a caso, con reguladores independientes y fuertes.

En esta línea, entre los desafíos del mercado digital, se plantea que las empresas operan a nivel mundial y que se sustentan en gran medida en activos intangibles difíciles de valorar, lo cual afecta la competitividad internacional y la fiscalidad, en tanto mucha de la normativa actual ha dejado de encajar, favoreciendo la elusión fiscal.[325]

Partiendo de esa base, la Comisión Europea realizó la Comunicación Nº 146 al Parlamento Europeo y al Consejo, destacando que la economía digital está transformando la forma en que se interactúa, en que se consume y en que se hacen negocios, pasando a ser una de las principales prioridades de la UE el mercado único digital, en tanto le permitirá mantenerse como líderes mundiales, brindando nuevas oportunidades para la innovación y ayudando a las empresas a crecer a escala mundial.

Destacan que las empresas digitales crecen mucho más que la economía en general, *"los ingresos medios anuales de las principales empresas digitales aumentaron aproximadamente un 14 %, frente a alrededor del 3 % en el caso de las empresas de ti y*

---

digital/conferencias/manifiesto-digital-de-telefonica-por-una-internet-abierta-y-segura-para-todos/ Consultado el 20 de febrero de 2019.

325 Comunicación de la Comisión Europea Nº 547 del 21 de setiembre de 2017.

telecomunicaciones y el 0,2 % en el caso de otras multinacionales", plantean la necesidad de establecer una fiscalidad justa y eficaz, actualizada, en el que "las actividades digitales se estimen por su justo valor y en el que puedan crecer empresas orientadas al sector digital disfrutando de un sector empresarial justo y predecible"[326].

Asimismo, señalan que si bien se viene trabajando en mejorar la equidad y la eficiencia de los sistemas fiscales, la rápida transformación de la economía por la digitalización ejerce nuevas presiones, siendo necesario asegurar la competencia, el emprendedurismo, atender los nuevos modelos de negocios y que las empresas tributen donde están ubicadas sus actividades económicas. Se quiere que las empresas digitales también contribuyan con sus impuestos en la medida que les corresponda.[327]

En paralelo, desde el año 2013 la Organización para la Cooperación y el Desarrollo Económico (OCDE) está trabajando en un Plan de Acción sobre la "Erosión de la base imponible y traslado de beneficios" o beps –por sus siglas en inglés–. El Plan contiene 15 líneas de acción y fue respaldado por la Cumbre del G20 de San Petersburgo de 2013.

En relación a los desafíos fiscales, en abril del 2018 se realizó un *informe provisional*[328] sobre los efectos fiscales de la digitalización de la economía. Se indica –entre otras cosas–: (i) que los países han acordado armonizar la determinación del criterio de sujeción y las reglas de atribución de beneficios, conceptos fundamentales relativos al reparto de la potestad tributaria entre jurisdicciones y a la determinación de la parte de los beneficios de las empresas multinacionales que estará sujeta a impuestos en una jurisdicción determinada; (ii) que hay países que consideran absolutamente necesario actuar con rapidez y adoptar medidas provisionales, como ser la aplicación de un impuesto especial a la prestación de ciertos servicios digitales efectuada bajo su jurisdicción que se aplicaría al importe bruto satisfecho como contraprestación a dichos servicios digitales. Mas no hay consenso, habiendo muchos países que se oponen a adoptar medidas provisionales, en tanto consideran que generaría riesgos y tendría efectos adversos; (iii) que teniendo en cuenta la disponibilidad de acceso a datos

326 https://ec.europa.eu/transparency/regdoc/rep/1/2018/ES/COM-2018-146-F1-ES-MAIN-PART-1.PDF Consultado el 20 de febrero de 2019.
327 http://europa.eu/rapid/press-release_IP-18-2041_es.htm Consultado el 20 de febrero de 2019.
328 https://www.oecd.org/tax/beps/resumen-desafios-fiscales-derivados-de-la-digitalizacion-informe-provisional-2018.pdf Consultado el 20 de febrero de 2019.

masivos, se reconoce la necesidad de intensificar la cooperación internacional entre las administraciones tributarias, principalmente para atender la economía colaborativa, la economía por encargo, así como para examinar las repercusiones fiscales de las nuevas tecnologías (criptomonedas, contabilidad distribuida o *blockchain*); (iv) que se reconoce como rasgos característicos de la economía digital: "lo que se ha dado en llamar «magnitud sin multitud», la fuerte dependencia de los activos intangibles y el papel de los datos y de la participación de los usuarios, incluidos los efectos de red"; mas se señala que hay diversos puntos de vista respecto a si esas características contribuyen a la creación de valor por parte de las empresas y en qué medida; (v) que la implementación de las medidas beps ya está en marcha en la mayoría de los países, sólo en la UE se han recaudado más de 3.000 millones de euros como consecuencias de la implementación de las nuevas Directrices Internacionales sobre iva/ibs; y (vi) que en relación al impuesto sobre sociedades (is) se han acometido importantes reformas, al tiempo que una de las medidas de la reforma fiscal estadounidense (gilti) establece la obligación de tributar por las rentas mundiales procedentes de activos intangibles sometidos a un tipo de gravamen reducido, al tiempo que muchas empresas multinacionales han adoptado medidas proactivas para realizar sus respectivas estructuras fiscales.

Más allá de las diversas posiciones, se acordó revisar el criterio de sujeción y las reglas de atribución de beneficios, en tanto se consideran fundamentales para determinar la potestad tributaria entre jurisdicciones y la forma en que se asignan los beneficios a las diferentes actividades desarrolladas por las empresas multinacionales.

Se subraya que llevará tiempo aproximar posiciones, diseñar e implementar una solución mundial, por lo que en algunos países ya se están tomando medidas. Vale destacar que no hay consenso acerca de la necesidad o conveniencia de adoptar medidas provisionales, al tiempo que son varios los países que se oponen a dichas medidas por considerar que generarán riesgos y tendrán efectos adversos como pueden ser repercusiones negativas en la inversión, la innovación y el crecimiento. Además, que podría generar sobreimposición, efectos distorsionadores de la producción, aumento de la carga fiscal soportada por consumidores y empresas, y unos costes de cumplimiento y gastos administrativos más elevados.[329]

329 https://www.oecd.org/tax/beps/resumen-desafios-fiscales-derivados-de-la-digitalizacion-informe-provisional-2018.pdf Consultado el 20 de febrero de 2019.

Sin perjuicio de lo anterior y de reconocer la necesidad de alcanzar una solución internacional, considerando la complejidad de la temática y la gran variedad de cuestiones que deben abordarse, paralelamente a los debates internacionales, en el entendido de que no puede esperarse hasta el 2020, la UE propuso dos directivas en marzo de 2018. La primera de corto plazo, mediante un impuesto provisional sobre los servicios digitales que grava los ingresos de determinados servicios digitales. La segunda, implica una reforma permanente de las normas del impuesto sobre sociedades, sobre la base del concepto de presencia digital significativa[330].

Por otra parte, es interesante señalar que en Estados Unidos en Junio del 2018 la Suprema Corte de Justicia resolvió el conocido caso llamado *¨Impuestos del milenio¨*, en donde se intentaba modificar el caso *Quill v. North Dakota* el cual dispuso que las compañías solo tenían que cobrar el impuesto a las ventas en los estados en donde se encontraban físicamente localizadas, donde tenían sus residencias o desde donde enviaban sus pedidos, no tributando así en los estados en donde prestaban sus servicios.

En el caso, el Estado de South Dakota (*South Dakota vs Wayfair*) planteó que cuando un consumidor compra bienes o servicios, el Estado impone un impuesto a las ventas, y quería saber cuándo se puede exigir a un vendedor de fuera del Estado que esté gravado por ese impuesto.

La Suprema Corte en su sentencia[331] señala que la regla de la presencia física ha sido muy criticada, en tanto debería centrarse en reglas apropiadas para el siglo XXI porque se aleja de la realidad económica y se traduce en importantes pérdidas de ingresos para los estados.

Hace referencia a la economía moderna con su tecnología de Internet, que la interpretación bajo Quill puede llevar a que una compañía pequeña con presencia física podría estar más gravada que una compañía grande con vendedores remotos, que la presencia física es artificial, y que la Cláusula de Comercio lo que busca –entre otras cosas- es poner a las empresas en igualdad de condiciones.

---

330 http://www.europarl.europa.eu/RegData/etudes/ATAG/2018/630327/EPRS_ATA(2018)630327_ES.pdf Consultado el 20 de febrero de 2019.

331 https://www.supremecourt.gov/opinions/17pdf/17-494_j4el.pdf Consultado el 20 de febrero de 2019.

Asimismo, hace mención a los dramáticos cambios tecnológicos y sociales acaecidos, que estamos en una economía cada vez más interconectada, que un negocio puede estar muy presente en un estado sin tener que estar físicamente en el mismo, no debiendo ignorar las conexiones virtuales.

Destaca que Internet ha cambiado la dinámica de la economía nacional, las ventas de comercio electrónico crece y se multiplica sin parar, en mucha más cantidad que el minorista tradicional.

En definitiva, la Suprema Corte señala que se establece un nexo cuando el contribuyente se beneficia de realizar negocios en esa jurisdicción, bastando con los contactos económicos y virtuales.

En suma, no cabe duda de los beneficios que la economía digital genera para todos, mas es esencial reconocer que genera múltiples cambios, siendo fundamental que se identifiquen los retos a fin de trabajar sobre los mismos, generando los ajustes y tomando las medidas que sean necesarias para que se pueda desarrollar el ecosistema digital y convivir con el mundo tradicional de la mejor forma.

VI. Consideraciones finales

Los servicios y aplicaciones digitales que se brindan a través de plataformas han generado una nueva economía, que tiene muchos beneficios, al tiempo que presenta múltiples desafíos.

La temática es de suma actualidad, tanto a nivel regional como nacional, se está trabajando y analizando cómo afrontar esta nueva realidad, buscando el desarrollo de la economía digital y la protección de los derechos fundamentales de las personas; al tiempo que se promueva la innovación y la inversión, controlando los riesgos, protegiendo la competencia, a los consumidores y usuarios.

Se procede a comentar sobre la regulación e iniciativas regulatorias existentes tanto en España como en Uruguay en relación a la temática; así como el impacto de esta nueva realidad en los derechos fundamentales.

CAPÍTULO VI: NUEVAS REGULACIONES PARA EL DESARROLLO DEL MERCADO DIGITAL: CASOS DE ESPAÑA Y URUGUAY

I. Introducción

No cabe duda de que con el desarrollo de las telecomunicaciones y de las nuevas tecnologías, se han desarrollado nuevos mercados que impactan en la economía, en la competencia, así como en los derechos de las personas.

Las plataformas electrónicas permiten prestar y comercializar diversos servicios y productos, en todo o en parte a través de Internet, cambiando la forma de consumir de los usuarios, generando gran impacto en todas las áreas de actividad y construyendo la economía digital.

La economía digital tiene muchos beneficios para las sociedades y para la economía, en tanto las formas cambian buscando atender las necesidades de la sociedad; mas al mismo tiempo presenta múltiples retos.

Identificar debidamente los diversos aspectos que pueden llegar a ser vulnerados, es esencial para poder trabajar sobre los mismos y alcanzar seguridad jurídica, innovación, desarrollo, investigación e inversión. Además de atender los derechos humanos, es fundamental trabajar sobre los siguientes aspectos:

a. La libre y sana competencia: aparecen nuevos actores que sustituyen y/o compiten con los actores tradicionales, pero que lo hacen en condiciones desiguales por la existencia de asimetrías regulatorias. Se plantea la necesidad de rever la regulación y de garantizar igualdad en las reglas de juego entre servicios similares, en tanto en muchos casos –como por ejemplo con los aspectos fiscales– las reglas no fueron pensadas para los nuevos supuestos.

b. Atender las regulaciones de los países, actualizar y eliminar aquello que sea necesario. Ocurre: (i) que las regulaciones vigentes responden a realidades diferentes, por lo que no son adecuadas; (ii) que por miedo o desconocimiento se solicitan múltiples requisitos y exigencias que no reflejan la realidad, ni las posibilidades, al tiempo que exceden el riesgo potencial que se quiere cubrir; (iii) que no hay claridad respecto a lo que rige, lo cual genera zonas grises, no queda claro si la actividad queda alcanzada o no por determinada regulación, ni la normativa aplicable.

c. Regular de una forma más inteligente, lo cual facilitará el desarrollo y diferenciará a los países. Aquellos que entiendan, atiendan y promuevan la nueva realidad, con una visión cabal, desarrollarán mejor el ecosistema generando más oportunidades para todos. Es esencial responder de una manera más inteligente, adecuada, evitando errores, ateniendo la necesidad y la realidad, de forma proporcional. Para lo cual debemos: (i) Aprender de las experiencias que ya tienen otros países, algunos tienen más camino transitado en la temática. (ii) Trabajar en conjunto, entender y dialogar entre los diversos actores del sector. (iii) Medir, controlar, así como revisar periódicamente las soluciones adoptadas.

Como señala Luciana Macedo[332], entre los impactos que genera la nueva realidad digital, se destacan los siguientes:

efectos de red: *"Las plataformas digitales conectan dos o más grupos de agentes, como consumidores y oferentes. El valor reside en la interacción de dichos grupos, que genera externalidades de red cruzadas. La participación es más atractiva para cada individuo cuántos más usuarios participen en la plataforma."*

Interoperabilidad: *"permite que las plataformas y las aplicaciones producidas por distintos desarrolladores puedan conectarse entre sí. Cuanto mayor la interoperabilidad entre plataformas, mayor es el valor de los productos y servicios ofrecidos a través de éstas."*

Algoritmos y uso de *big data*: *"El uso del big data a través de algoritmos disminuye las asimetrías de información entre consumidores y proveedores. Los consumidores pueden comparar precios, calidad, tiempos de envío, etc. Así, pueden tomar mejores decisiones de compra. Por su parte, los proveedores usan la información para conocer mejor a los consumidores y realizar ofertas de acuerdo a sus necesidades y gustos y también para conocer mejor a sus competidores."* (…) *"Pero, el big data y el uso de algoritmos pueden tener como efecto una reducción de la competencia. La información podría ser una barrera a la entrada de competidores. Los algoritmos pueden operar como facilitadores de la colusión. A través de los algoritmos pueden surgir nuevas formas de coordinación entre proveedores ya que facilitan la manipulación de la información."*

[332] MACEDO, LUCIANA, "Economía Digital y competencia" en *Estudios sobre los Desafíos Jurídicos ante la Digitalización*, Universidad de Montevideo, 2019. pp. 257 y ss.

Efectos de la economía colaborativa: *"Estos modelos de negocio tienen como efecto positivo una mejora en la asignación de recursos." (...) "Además, estos modelos de negocio reducen la asimetría de información. (...) Los sistemas de valoración permiten generar reputación y confianza. Otro efecto positivo de este tipo de modelos es la disminución de los costos de transacción: menores costos de búsqueda y de información." "Pero, la economía colaborativa, puede generar determinadas dinámicas que lleven a la concentración y al poder del mercado. La tendencia a la concentración en los mercados digitales es favorecida por las externalidades de red y las economías de escala."*

La economía digital impacta en los sectores tradicionales, así como en el mercado del trabajo y en los derechos fundamentales de las personas, entre otras cosas, generando que la temática se ponga en las agendas públicas y que se empiece a analizar la regulación de múltiples aspectos para poder responder de la mejor forma a la nueva realidad.

Entre los principales problemas que enfrentan las autoridades se destacan: (i) Determinar la jurisdicción: al ser virtuales muchas veces es difícil definir los puntos geográficos físicos; (ii) Definir el mercado relevante: en general son muy dinámicos, puede ser que haya más de un mercado involucrado, que se diluyan las diferencias entre mercados diferentes; (iii) Evaluar el poder del mercado: muchos servicios no tienen precio establecido, se supone que son gratis o tienen beneficios muy bajos, por lo que se sugiere analizar otros aspectos, ya sean directos o indirectos; (iv) Colusión a través de algoritmos, nuevas formas de coordinación, se generan muchas zonas grises, generándose mecanismos automáticos que genera políticas comunes y contralor de la competencia; y (v) entender la tecnología, revisar las definiciones y normativas vigentes, asegurarse de que se sigan respetando los derechos y garantías.[333]

Por otra parte, como hemos señalado, una de las características de la era digital en la que estamos viviendo es la velocidad. En este sentido, como señala Pilar Brito: *"Hasta el momento cualquier compañía, e incluso más las del rubro financiero, tenían un crecimiento predecible y prácticamente siempre era exponencial. Comienzan siendo pequeñas, en cuyo caso el regulador no se detiene demasiado tiempo en ellas ya que la influencia que tienen en el mercado es muy menor –a esto se lo conoce como "too small to care"–. El regulador podía predecir la influencia de la compañía en el mercado por*

[333] MACEDO, LUCIANA, obra citada, pp. 257 y ss.

toda su trayectoria, pasando a ser lo suficientemente grande y/o influyente en el mercado como para ignorar, punto que se lo conoce como "too big to fail".[334]

Ahora bien, dado el tamaño de la inversión y las implicaciones competitivas derivadas de las Fintech, el regulador ya no puede seguir teniendo los mismos procesos que tenía antes. Deben cambiar los métodos utilizados para identificar a tiempo el futuro de estos nuevos actores. En Asia, continente en el cual las Fintech y su regulación está bastante desarrollada, sucedió el paradigmático caso de Yu'e Bao una Fintech china que paso de ser una compañía too small to care a too big to fail en tan solo nueve meses (pasando de USD 0 a USD 90 mil millones). A la industria financiera tradicional le costó más de siete décadas en lograr ese mismo crecimiento.[335 ,,336]

Considerando todo lo expuesto, se reconoce que cada vez es más difícil poder prever, por lo que se apunta con gran énfasis en cambiar la forma de regular y empezar a hacer regulaciones flexibles, temporales, basadas en el diálogo, para poder probar en ambientes controlados, aprender de la experiencia, del contexto y tomar las medidas en función de los resultados. En este sentido, se habla de avanzar hacia una regulación más inteligente, al tiempo que se plantea con mayor intensidad la importancia de analizar las regulaciones existentes a efectos de rever si se ajusta a la nueva realidad, si atienden debidamente las necesidades, a fin de actualizar y de dejar sin efecto lo que sea necesario.

Lo anterior es fundamental para promover la innovación, dando seguridad. Los grises o la falta de claridad y de previsibilidad puede afectar mucho al desarrollo. Un claro ejemplo de los efectos negativos que puede haber por la falta de claridad regulatoria se ve en los Estados Unidos respecto a la regulación de las ICOs para determinar si son Securities o Utilities. En caso de que sean Securities deben cumplir con mayores requisitos legales, no se ha tenido seguridad sobre el punto, lo cual ha derivado en que varias empresas sean sancionadas por la SEC por considerar que

---

334 BID: Sandbox Regulatorio en America Latina y en el Caribe para el ecosistema Fintech y el sistema financiero https://publications.iadb.org/bitstream/handle/11319/8795/Sandbox-Regulatorio-en-America-Latina-y-el-Caribe-para-el-ecosistema-Fintech-y-el-sistema-financiero-vf.pdf Consultado el 20 de enero de 2019.

335 ARNER, DOUGLAS, BARBERIS, JANOS, BUCKLEY, ROSS, "The Evolution of Fintech: A New Post-Crisis Paradigm?", Hong Kong University en https://hub.hku.hk/bitstream/10722/221450/1/Content.pdf Consultado el 20 de enero de 2019.

336 BRITO, MARÍA PILAR, "Fintech: la reconceptualización de la regulación financiera. Ejemplos del derecho comparado" en *Estudios sobre los Desafíos Jurídicos ante la Digitalización"*, obra citada, pp. 345 y ss.

estaban emitiendo valores y no estaban cumpliendo con las regulaciones correspondientes. Considerando los diversos casos que se han ido planteando, Estados Unidos está analizando cada caso en concreto y sometiendo cada supuesto al llamado "Howie test" creado por la Suprema Corte de Justicia para determinar a qué regulación se debe someter. Se analizan cuatro aspectos: (1) si es una inversión de dinero o de activos diferentes al dinero, (2) si hay una expectativa de obtener ganancias por la inversión, (3) si en la inversión quienes participan ponen dinero o activos de manera conjunta para invertir en el proyecto, y (4) si cualquier ganancia viene por el esfuerzo de un promotor o de una tercera parte, estando fuera del control de los inversores. Si se cumplen esas condiciones, probablemente la inversión sea considerada como un security, debiendo someterse a la regulación específica que corresponda[337].

En este sentido, como se adelantó, hay diversas iniciativas y desafíos, tanto a nivel global, regional como nacionales, la realidad es que es muy difícil poder prever todos los problemas que van a ir surgiendo. Además, un gran desafío es regular adecuadamente, sin afectar la innovación y el desarrollo, y a tiempo, a fin de que no se afecten otros derechos.

Lo anterior se está planteando en diversos ámbitos de actividad.

A continuación comentaremos sobre la regulación que rige o que se está analizando en España y en Uruguay, vinculada a servicios en la sociedad de la información, el comercio electrónico, las plataformas electrónicas y diversos aspectos relacionados con las *Fintech*, como son los pagos y el dinero electrónicos, las monedas digitales y las plataformas de financiación colectiva.

(II) Regulación en España

España cuenta con regulación sobre la materia desde hace más de 15 años. Sin perjuicio, como se ha reiterado en múltiples ocasiones, los cambios en esta área de actividad es constante, por lo que la actualización normativa, así como la regulación de nuevos aspectos es permanente.

(II.1) Servicios de la Sociedad de la Información y de Comercio Electrónico.

Conforme a lo establecido en la Directiva 98/34/CE, modificada por la Directiva 98/48/CE, se entiende por "Servicios de la sociedad de la información" a *"todo servicio*

[337] What Is the Howey Test?, https://consumer.findlaw.com/securities-law/what-is-the-howey-test.html Consultado el 15 de enero de 2019.

prestado normalmente a cambio de una remuneración, a distancia, por vía electrónica y a petición individual de un destinatario de servicios"[338]. En esta línea, consideran que "a distancia" implica que las partes no están presentes ante sí, y "por vía electrónica" refiere a *"un servicio enviado desde la fuente y recibido por el destinatario mediante equipos electrónicos de tratamiento (incluida la compresión digital) y de almacenamiento de datos y que se transmite, canaliza y recibe enteramente por hilos, radio, medios ópticos o cualquier otro medio electromagnético*[339]*".*

El Parlamento Europeo y del Consejo aprobó el 8 de junio de 2000 la Directiva 2000/31/CE, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el Mercado interior.

Como surge de la exposición de motivos, se considera que "*El desarrollo del comercio electrónico en la sociedad de la información ofrece importantes oportunidades para el empleo en la Comunidad, especialmente para las pequeñas y medianas empresas, que facilitará el crecimiento de las empresas europeas, así como las inversiones en innovación, y también puede incrementar la competitividad de la industria europea, siempre y cuando Internet sea accesible para todos*[340]*"*

Pero, entre otras cosas, se identifica que para que se pueda desarrollar, es esencial garantizar la seguridad jurídica y dar confianza a los consumidores, para lo cual se busca asegurar la libre circulación de los servicios de la sociedad de la información entre los Estados miembros, de conformidad con el principio de proporcionalidad.

No se puede restringir la libertad para prestar los servicios de la sociedad de la información. Sin perjuicio, se pueden establecer determinadas medidas siempre que: (i) sean necesarias por motivos de orden público, para proteger la salud pública, para la seguridad pública, así como para proteger a los consumidores e inversores; (ii) el servicio vaya en contra de dichos motivos o constituya un riesgo serio y grave para dichos objetivos; y (iii) que sean proporcionados a los objetivos. Se prevé que antes de adoptar medidas, el Estado que vaya a tomarlas, debe de haber requerido previamente al otro Estado que adopte soluciones y no las haya tomado, y que notifique previamente a dicho Estado y a la Comisión. Por otra parte, se prevén casos de urgencia, los cuales

[338] Directiva 98/48/CE, https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex:31998L0048 Consultado el 15 de enero de 2019.
[339] Ibídem
[340] Considerando (2) de la Directiva 2000/31/CE.

deberán ser notificados previamente. En todos los casos, la Comisión examinará la compatibilidad de las medidas adoptadas, pudiendo requerir que sean dejadas sin efecto[341].

Entre los principios que rigen la actuación se destacan los siguientes:

No autorización previa: los servicios no deben someterse a autorización previa ni a ningún otro requisito[342].

Información general exigida: los prestadores deben garantizar a los destinatarios de los servicios y a las autoridades acceder fácilmente a información básica. Como mínimo a la siguiente información: (a) nombre del prestador de servicios; (b) dirección geográfica donde está establecido el prestador de los servicios; (c) formas para contactarlo rápidamente; (d) identificación en el registro mercantil u otro registro similar; (e) si la actividad a prestarse requiere autorización específica, los datos de la autoridad de supervisión que corresponda; (f) si se trata de una profesión regulada, se requieren los datos del colegio o institución similar, el título expedido, el Estado y referencia a las normas profesionales aplicables; (g) si el prestador ejerce una actividad gravada por el impuesto por el valor añadido (IVA); y (h) que el precio se indique claramente, indicando si están o no incluidos los impuestos[343].

Por otra parte, se prevé que las comunicaciones comerciales deben estar bien identificadas, individualizando a las personas físicas o jurídicas en nombre de quién se realizan las mismas. Asimismo, se deben identificar las ofertas, promociones, así como los concursos o juegos promocionales[344].

Interesa señalar que los Estados miembros tienen que permitir la celebración de contratos por vía electrónica, garantizando no entorpecer la utilización de los contratos por vía electrónica. Sin perjuicio, se admite que no se aplique para contratos: (i) relativos a derechos en materia inmobiliaria, excepto los alquileres; (ii) que requieran la intervención de los tribunales, autoridades públicas o profesionales que ejerzan función pública; (iii) de crédito o caución y las garantías brindadas por personas que actúan por

[341] Artículo 3 de la Directiva 2000/31/CE.
[342] Artículo 4 de la Directiva 2000/31/CE.
[343] Artículo 5 de la Directiva 2000/31/CE.
[344] Artículo 6 de la Directiva 2000/31/CE.

motivos ajenos a su actividad económica, negocio o profesión; y (iv) en materia de derecho de familia o sucesiones[345].

Importa especialmente lo señalado en el artículo 12 de la Directiva 2000/31/CE en tanto indica que los servicios de la sociedad de la información que consistan en la mera transmisión de datos facilitados por el destinatario del servicio o en facilitar el acceso a una red de comunicaciones, no se puede considerar como responsable de dichos datos al prestador de los servicios, siempre que: (i) no haya originado él la transmisión, (ii) no elija al destinatario de la misma, y (iii) no seleccione ni modifique el contenido transmitido.

En esta línea, se prevé que el prestador de un servicio de la sociedad de la información que consista en transmitir por una red de comunicaciones datos facilitados por el destinatario del servicio, no puede ser considerado como responsable del almacenamiento de la información, siempre que: (i) no la modifique, (ii) cumpla con las condiciones de acceso, (iii) respete las normas de actualización, (iv) no interfiera en la utilización de tecnología para obtener datos sobre la utilización de la información, y (v) actúe con prontitud para retirar la información o hacer imposible el acceso a ella, en cuanto tenga conocimiento efectivo del hecho de que la información ha sido retirada, de que se ha imposibilitado el acceso a ella, o de que un tribunal o autoridad administrativa haya ordenado retirarla o impedido el acceso[346].

Por otra parte, en lo que respecta al servicio de almacenamiento de datos, se prevé que el prestador de dicho servicio no puede ser considerado responsable por los mismos, salvo que: (i) tenga conocimiento efectivo de que la actividad a la que refiere la información es ilícita, (ii) tenga conocimiento de hechos o circunstancias que revelen la ilicitud de la actividad o de la información, (iii) no actúe con prontitud para retirar los datos o imposibilitar el acceso en cuanto tenga conocimiento de las ilicitudes mencionadas[347].

Finalmente, corresponde destacar que los Estados partes no pueden imponer a los prestadores de servicios la obligación general de supervisar los datos que transmiten o que almacenen, ni la obligación de realizar búsquedas activas de hechos o

[345] Artículo 9 de la Directiva 2000/31/CE.
[346] Artículo 13 de la Directiva 2000/31/CE.
[347] Artículo 14 de la Directiva 2000/31/CE.

circunstancias que puedan indicar actividades ilícitas[348]. Sin perjuicio, sí se podrá prever que comuniquen con prontitud a las autoridades públicas competentes los presuntos datos o actividades ilícitas realizadas por usuarios de sus servicios, así como la obligación de comunicar, a solicitud de las autoridades competentes, información que les permita identificar a los destinatarios de sus servicios[349].

Teniendo en cuenta lo expuesto, España aprobó la Ley de servicios de la sociedad de la información y de comercio electrónico (LSSI), Ley Nº 34/2002, con el objetivo de regular el régimen jurídico de los servicios de la sociedad de la información y de la contratación por vía electrónica, previendo, entre otras cosas: (i) las obligaciones de los prestadores de servicios, (ii) las comunicaciones comerciales, (iii) la información previa y posterior a la celebración de contratos electrónicos, (iv) las condiciones de validez y eficacia.

La LSSI define ¨Servicios de la Sociedad de la Información" o "Servicios" como *"todo servicio prestado normalmente a título oneroso, a distancia, por vía electrónica y a petición individual del destinatario", "comprende también los servicios no remunerados por sus destinatarios, en la medida en que constituyan una actividad económica para el prestador de servicios"*. Son servicios de la sociedad de la información*: "(1) la contratación de bienes o servicios por vía electrónica, (2) la organización y gestión de subastas por medios electrónicos o de mercados y centros comerciales virtuales, (3) la gestión de compras en la red por grupos de personas, (4) el envío de comunicaciones comerciales y (5) el suministro de información por vía telemática[350]".*

Esta norma se debe complementar con otras disposiciones legales, como ser la Ley Nº 7/1996 de Ordenación del Comercio Minorista, la Ley Nº 7/1998 de Condiciones Generales de la Contratación, la Ley Nº 56/2007 de Medidas de Impulso de la Sociedad de la Información, la Ley Nº 25/2013 de Impulso a la Facturación electrónica, así como el Real Decreto Nº 1/2007 por el que se aprueba el texto refundido de la Ley General para la Defensa de los Consumidores y Usuarios.

[348] Artículo 15 de la Directiva 2000/31/CE.
[349] Ibídem.
[350] Anexo de la Ley de servicios de la sociedad de la información y de comercio electrónico, Nº 34/2002.

La prestación de los servicios de la sociedad de la información se rige por los siguientes principios: (i) no sujeción a autorización previa: no alcanza a aquellos regímenes de autorización que no tengan por objeto exclusivo y específico la prestación por vía electrónica de los correspondientes servicios[351]; (ii) libre prestación de los servicios: sin que pueda establecerse ningún tipo de restricción por causas derivadas del ámbito de aplicación, con excepción de los casos expresamente previstos[352] en los

[351] Artículo 6 de la Ley 34/2002.

[352] Artículo 3 y 8 de la Ley 34/2002.

El artículo 3 prevé lo siguiente: "*Artículo 3. Prestadores de servicios establecidos en otro Estado miembro de la Unión Europea o del Espacio Económico Europeo.*

1. Sin perjuicio de lo dispuesto en los artículos 7.1 y 8, esta Ley se aplicará a los prestadores de servicios de la sociedad de la información establecidos en otro Estado miembro de la Unión Europea o del Espacio Económico Europeo cuando el destinatario de los servicios radique en España y los servicios afecten a las materias siguientes:

a) Derechos de propiedad intelectual o industrial.

b) Emisión de publicidad por instituciones de inversión colectiva.

c) Actividad de seguro directo realizada en régimen de derecho de establecimiento o en régimen de libre prestación de servicios.

d) Obligaciones nacidas de los contratos celebrados por personas físicas que tengan la condición de consumidores

e) Régimen de elección por las partes contratantes de la legislación aplicable a su contrato.

f) Licitud de las comunicaciones comerciales por correo electrónico u otro medio de comunicación electrónica equivalente no solicitadas.

2. En todo caso, la constitución, transmisión, modificación y extinción de derechos reales sobre bienes inmuebles sitos en España se sujetará a los requisitos formales de validez y eficacia establecidos en el ordenamiento jurídico español.

3. Los prestadores de servicios a los que se refiere el apartado 1 quedarán igualmente sometidos a las normas del ordenamiento jurídico español que regulen las materias señaladas en dicho apartado.

4. No será aplicable lo dispuesto en los apartados anteriores a los supuestos en que, de conformidad con las normas reguladoras de las materias enumeradas en el apartado 1, no fuera de aplicación la ley del país en que resida o esté establecido el destinatario del servicio."

El artículo 8 dispone restricciones a la prestación de servicios y procedimiento de cooperación intracomunitario: **"***1. En caso de que un determinado servicio de la sociedad de la información atente o pueda atentar contra los principios que se expresan a continuación, los órganos competentes para su protección, en ejercicio de las funciones que tengan legalmente atribuidas, podrán adoptar las medidas necesarias para que se interrumpa su prestación o para retirar los datos que los vulneran. Los principios a que alude este apartado son los siguientes:*

a) La salvaguarda del orden público, la investigación penal, la seguridad pública y la defensa nacional.

b) La protección de la salud pública o de las personas físicas o jurídicas que tengan la condición de consumidores o usuarios, incluso cuando actúen como inversores.

c) El respeto a la dignidad de la persona y al principio de no discriminación por motivos de raza, sexo, religión, opinión, nacionalidad, discapacidad o cualquier otra circunstancia personal o social, y

d) La protección de la juventud y de la infancia.

e) La salvaguarda de los derechos de propiedad intelectual.

En la adopción y cumplimiento de las medidas de restricción a que alude este apartado se respetarán, en todo caso, las garantías, normas y procedimientos previstos en el ordenamiento jurídico para proteger los derechos a la intimidad personal y familiar, a la protección de los

artículos 3 y 8 de la Ley Nº 34/2002[353]. Respecto a las restricciones, la Ley prevé la posibilidad de interrumpir la prestación o retirar datos, en caso de que un determinado

datos personales, a la libertad de expresión o a la libertad de información, cuando éstos pudieran resultar afectados.
En todos los casos en los que la Constitución y las leyes reguladoras de los respectivos derechos y libertades así lo prevean de forma excluyente, sólo la autoridad judicial competente podrá adoptar las medidas previstas en este artículo, en tanto garante del derecho a la libertad de expresión, del derecho de producción y creación literaria, artística, científica y técnica, la libertad de cátedra y el derecho de información.
2. Los órganos competentes para la adopción de las medidas a que se refiere el apartado anterior, con el objeto de identificar al responsable del servicio de la sociedad de la información que está realizando la conducta presuntamente vulneradora, podrán requerir a los prestadores de servicios de la sociedad de la información la cesión de los datos que permitan tal identificación a fin de que pueda comparecer en el procedimiento. Tal requerimiento exigirá la previa autorización judicial de acuerdo con lo previsto en el apartado primero del artículo 122 bis de la Ley reguladora de la Jurisdicción contencioso-administrativa. Una vez obtenida la autorización, los prestadores estarán obligados a facilitar los datos necesarios para llevar a cabo la identificación.
3. La adopción de restricciones a la prestación de servicios de la sociedad de la información provenientes de prestadores establecidos en un Estado de la Unión Europea o del Espacio Económico Europeo distinto a España deberá seguir el procedimiento de cooperación intracomunitario descrito en el siguiente apartado de este artículo, sin perjuicio de lo dispuesto en la legislación procesal y de cooperación judicial.
4. Cuando un órgano competente acuerde, en ejercicio de las competencias que tenga legalmente atribuidas, y de acuerdo con lo dispuesto en el párrafo a) del apartado 4 del artículo 3 de la Directiva 2000/31/CE, establecer restricciones que afecten a un servicio de la sociedad de la información que proceda de alguno de los Estados miembros de la Unión Europea o del Espacio Económico Europeo distinto de España, dicho órgano deberá seguir el siguiente procedimiento:
a) El órgano competente requerirá al Estado miembro en que esté establecido el prestador afectado para que adopte las medidas oportunas. En el caso de que no las adopte o resulten insuficientes, dicho órgano notificará, con carácter previo, a la Comisión Europea o, en su caso, al Comité Mixto del Espacio Económico Europeo y al Estado miembro de que se trate las medidas que tiene intención de adoptar.
b) En los supuestos de urgencia, el órgano competente podrá adoptar las medidas oportunas, notificándolas al Estado miembro de procedencia y a la Comisión Europea o, en su caso, al Comité Mixto del Espacio Económico Europeo con la mayor brevedad y, en cualquier caso, como máximo, en el plazo de quince días desde su adopción. Así mismo, deberá indicar la causa de dicha urgencia.
Los requerimientos y notificaciones a que alude este apartado se realizarán siempre a través del órgano de la Administración General del Estado competente para la comunicación y transmisión de información a las Comunidades Europeas.
5. Los órganos competentes de otros Estados Miembros de la Unión Europea o del Espacio Económico Europeo podrán requerir la colaboración de los prestadores de servicios de intermediación establecidos en España en los términos previstos en el apartado 2 del artículo 11 de esta ley si lo estiman necesario para garantizar la eficacia de las medidas de restricción que adopten al amparo del apartado anterior.
6. Las medidas de restricción que se adopten al amparo de este artículo deberán, en todo caso, cumplir las garantías y los requisitos previstos en los apartados 3 y 4 del artículo 11 de esta ley."

[353] Artículo 7 de la Ley Nº 34/2002.

servicio de la sociedad de la información atente contra alguno de los siguientes principios:

"a) La salvaguarda del orden público, la investigación penal, la seguridad pública y la defensa nacional.

b) La protección de la salud pública o de las personas físicas o jurídicas que tengan la condición de consumidores o usuarios, incluso cuando actúen como inversores.

c) El respeto a la dignidad de la persona y al principio de no discriminación por motivos de raza, sexo, religión, opinión, nacionalidad, discapacidad o cualquier otra circunstancia personal o social,

d) La protección de la juventud y de la infancia.

e) La salvaguarda de los derechos de propiedad intelectual.[354]*"*

Entre las diversas obligaciones que tiene el prestador de los servicios se prevé:

Que está obligado a permitir acceder por medios electrónicos, de forma permanente, fácil, directa y gratuita, a la siguiente información:

"Su nombre o denominación social; su residencia o domicilio o, en su defecto, la dirección de uno de sus establecimientos permanentes en España; su dirección de correo electrónico y cualquier otro dato que permita establecer con él una comunicación directa y efectiva.

Los datos de su inscripción en el Registro Mercantil en el que, en su caso, se encuentren inscritos o de aquel otro registro público en el que lo estuvieran para la adquisición de personalidad jurídica o a los solos efectos de publicidad.

En el caso de que su actividad estuviese sujeta a un régimen de autorización administrativa previa, los datos relativos a dicha autorización y los identificativos del órgano competente encargado de su supervisión.

Si ejerce una profesión regulada deberá indicar:

Los datos del Colegio profesional al que, en su caso, pertenezca y número de colegiado.

El título académico oficial o profesional con el que cuente.

[354] Artículo 8 de la Ley Nº 34/2002.

El Estado de la Unión Europea o del Espacio Económico Europeo en el que se expidió dicho título y, en su caso, la correspondiente homologación o reconocimiento.

Las normas profesionales aplicables al ejercicio de su profesión y los medios a través de los cuales se puedan conocer, incluidos los electrónicos.

El número de identificación fiscal que le corresponda.

Cuando el servicio de la sociedad de la información haga referencia a precios, se facilitará información clara y exacta sobre el precio del producto o servicio, indicando si incluye o no los impuestos aplicables y, en su caso, sobre los gastos de envío.

Los códigos de conducta a los que, en su caso, esté adherido y la manera de consultarlos electrónicamente. [355]*"*

Por otra parte, tienen deber de colaborar con los órganos competentes[356], así como de informar: (i) *"sobre los diferentes medios de carácter técnico que aumenten los niveles de seguridad de la información y permitan, entre otros, la protección frente a virus informáticos y programas espía, y la restricción de los correos electrónicos no deseados*[357]", (ii) sobre las medidas de seguridad que apliquen para prestar los servicios, (iii) *"sobre las herramientas existentes para el filtrado y restricción del acceso a determinados contenidos y servicios en Internet no deseados o que puedan ser nocivos para la juventud y la infancia*[358]", y (iv) sobre las posibles responsabilidades en que pueden incurrir por el uso de Internet con fines ilícitos[359].

El régimen de responsabilidad tiene especial interés, en tanto como se verá en el capítulo vinculado con la libertad de expresión, los prestadores de servicios de la sociedad de la información están sujetos a responsabilidad civil, penal y administrativa, y por las actividades de intermediación[360]. Se tiene que atender lo dispuesto en los artículos 14, 15, 16 y 17 de la Ley Nº 34/2002, la cual identifica cuatro supuestos diferentes. El primer supuesto es relacionado con la responsabilidad de los operadores de redes y proveedores de acceso. El segundo supuesto es vinculado con los prestadores

[355] Artículo 10, numeral 1, de la Ley 34/2002.
[356] Artículo 11 de la Ley 34/2002.
[357] Artículo 12bis.1 de la Ley 34/2002.
[358] Artículo 12bis.3 de la Ley 34/2002.
[359] Artículo 12bis .4 de la Ley 34/2002.
[360] Se prevé que los servicios de intermediación *"son aquellos por los que se facilita la prestación o utilización de otros servicios de la sociedad de la información o el acceso a la información"* (Anexo a la Ley de servicios de la sociedad de la información y de comercio electrónico).

de servicios que realizan copia temporal de los datos solicitados por los usuarios. El tercer supuesto es sobre los prestadores de servicios de alojamiento o de almacenamiento de datos; y el último supuesto es relacionado a los prestadores de servicios que faciliten enlaces a contenidos o instrumentos de búsqueda.

Procedemos a desarrollar cada uno.

Los operadores de redes de telecomunicaciones y proveedores de acceso no serán responsables por la información transmitida cuando prestan servicios de intermediación, que consistan en transmitir por una red de telecomunicaciones datos o en facilitar acceso a la red. Salvo si ellos originaron la transmisión, modificaron los datos, los seleccionaron o eligieron a los destinatarios. Esta actividad incluye el almacenamiento automático, provisional y transitorio de los datos, siempre que sea para la transmisión por la red de telecomunicaciones y que la duración sea la razonablemente necesaria para tal fin[361].

Los prestadores de servicios que transmitan por una red de telecomunicaciones datos facilitados por un destinatario del servicio y los almacenen en sus sistemas de forma automática, provisional y temporal con la finalidad de hacer más eficaz su transmisión a otros destinatarios; no serán responsables por el contenido de esos datos, ni por la reproducción temporal de los mismos. Siempre que: a) no los modifiquen; b) permitan el acceso sólo a los destinatarios que cumplan con las condiciones establecidas; c) respetan las normas para la actualización; d) no interfieran en la utilización de la tecnología con el fin de obtener datos sobre la utilización, y e) retiren la información almacenada o imposibiliten el acceso a ella, en cuanto tengan conocimiento efectivo de: que ha sido retirada del lugar de la red en que se encontraba inicialmente, que se ha imposibilitado el acceso a ella, o que un tribunal u órgano administrativo competente ha ordenado retirarla o impedir que se acceda a ella[362].

Los prestadores de servicios de alojamiento o almacenamiento de datos no serán responsables por la información que almacenen a petición del destinatario. Siempre que: (a) no tengan conocimiento efectivo de que la actividad o la información almacenada es ilícita o que lesiona bienes o derechos susceptibles de indemnización, o (b) si tienen

[361] Artículo 14 de la Ley Nº 34/2002.
[362] Artículo 15 de la Ley Nº 34/2002.

conocimiento, actúen con diligencia para retirar los datos o imposibiliten el acceso a ellos[363].

Los prestadores de servicios que faciliten enlaces a contenidos o instrumentos de búsqueda, no serán responsables por la información a la que se dirijan a los destinatarios de los servicios. Siempre que: (a) no tengan conocimiento efectivo de que la actividad o la información es ilícita o de que lesiona bienes o derechos susceptibles de indemnización, o (b) si tienen conocimiento, actúen con diligencia para suprimir o dejar sin utilidad el enlace[364].

Determinar el "conocimiento efectivo" resulta esencial para establecer la responsabilidad. Conforme a lo previsto en los artículos 16 y 17 de la Ley 34/2002, se entiende que se configura el supuesto cuando un *"órgano competente haya declarado la ilicitud de los datos, ordenado su retirada o que se imposibilite el acceso a los mismos, o se hubiera declarado la existencia de la lesión, y el prestador conociera la correspondiente resolución, sin perjuicio de los procedimientos de detección y retirada de contenidos que los prestadores apliquen en virtud de acuerdos voluntarios y de otros medios de conocimiento efectivo que pudieran establecerse.*[365]"

En relación a este aspecto, es interesante señalar que el Tribunal Europeo de Derechos Humanos (TEDH) ha señalado sobre la responsabilidad de los portales de noticias por los contenidos publicados en los mismos: *"que el administrador de un portal de noticias en internet tiene la consideración de editor y, en consecuencia, responsabilidad directa por los contenidos publicados por los lectores. Es decir, asimila, a estos efectos, los portales de noticias de internet con los medios de comunicación tradicionales y les impone la llamada "culpa in vigilando".*

El hecho de que en este caso el portal de noticias tuviera un sistema de detección y retirada de comentarios de contenido obsceno, no le eximió de responsabilidad frente a los contenidos difamatorios de los lectores.[366]"

[363] Artículo 16 de la Ley Nº 34/2002.
[364] Artículo 17 de la Ley Nº 34/2002.
[365] Artículos 16 y 17 inciso tercero del numeral 1, de la Ley 34/2002.
[366] Comentario del Departamento de Telecomunicaciones y Media del Estudio Garrigues sobre la Sentencia del TEDH sobre la responsabilidad de los foros de Internet (Caso Delfi AS v. Estonia). URL: http://blog.garrigues.com/sentencia-del-tedh-sobre-la-responsabilidad-de-los-foros-de-internet-caso-delfi-as-v-estonia Consultado el 10 de julio de 2019.

¨El régimen de exención de responsabilidad de los intermediarios no impide la adopción por parte de las autoridades competentes de órdenes que exijan la terminación o eviten la comisión de una infracción, incluidas la supresión de información ilícita o la inhabilitación del acceso a la misma. Por tanto, la limitación de responsabilidad de los intermediarios depende de si estos tienen o no conocimiento efectivo. La falta de concreción de este concepto da lugar en la práctica a cierto grado de inseguridad jurídica. De acuerdo con la LSSI, sólo existirá conocimiento efectivo cuando un órgano competente haya declarado la ilicitud de los datos, ordenando su retirada o que se imposibilite el acceso a los mismos, o se hubiera declarado la existencia de la lesión, y el prestador conociera la correspondiente resolución, sin perjuicio de los procedimientos de detección y retirada de contenidos que los prestadores apliquen en virtud de acuerdos voluntarios y de otros medios de conocimiento efectivo que pudieran establecerse[367]¨

Sin perjuicio, como surge de la Sentencia del Tribunal Supremo, Sala de lo Civil, STS 69/2014, no hay unanimidad respecto a qué significa "conocimiento efectivo". Conforme a lo establecido en la Directiva 2000/31/CE y en los artículos 13.1 y 16 de la Ley 34/2002. Hay principalmente dos interpretaciones doctrinales del concepto "conocimiento efectivo". *"Una primera, cuyos argumentos principales se encuentran en los antecedentes legislativos y pre legislativos de la ley y en su propia literalidad, y viene a sostener que no habiéndose establecido legal ni reglamentariamente otros medios de conocimiento y a falta de acuerdos voluntarios sobre procedimientos de detección y retirada, sólo podrá afirmarse la concurrencia de "conocimiento efectivo" en presencia de una previa resolución de un órgano competente acerca de la ilicitud de los datos en cuestión. La segunda considera que la Directiva de que procede la Ley -que emplea el metro del "conocimiento efectivo" para la exención de responsabilidad penal y el de "conocimiento de hechos o circunstancias por los que la actividad o la información revele su carácter ilícito" para la que atañe a la responsabilidad civil-, el párrafo mencionado tiene naturaleza meramente ejemplificativa y no excluye que pueda probarse la existencia de "conocimiento efectivo" de cualquier otra manera.*[368]"

Por otra parte la LSSI también regula otros aspectos que se consideran fundamentales para el desarrollo de la sociedad de la información y del comercio

[367] SIGUENZA, ALICIA, ¨La libertad de expresión en Internet¨ en *El Derecho De Internet*, Editorial Atelier, 2016, pp. 67 y ss.
[368] Sentencia del Tribunal Supremo, Sala de lo Civil, STS 69/2014.

electrónico, como son: Impulsar la elaboración y aprobación de códigos de conducta voluntarios. Por parte de las corporaciones, asociaciones u organizaciones comerciales, profesionales y de los consumidores, que traten, entre otros temas, sobre los procedimiento para detectar contenidos ilícitos, para proteger a los consumidores frente a comunicaciones comerciales no solicitadas, así como aspectos vinculados a la resolución de conflictos que surjan en la prestación de estos servicios.[369]

Las comunicaciones comerciales por vía electrónica deben someterse a la normativa específica, y atender lo dispuesto en la regulación sobre protección de datos personales. Se exige que las mismas se identifiquen claramente como tales, así como a las personas físicas o jurídicas de quien las realiza. De la misma forma, se requiere que se identifiquen los supuestos de ofertas promocionales, previa autorización y cumplimiento de los requisitos que correspondan, estableciendo fácilmente, de forma clara e inequívoca las condiciones de acceso y de participación. Por otra parte, se prohíbe el envío de comunicaciones comerciales disimulando u ocultando la identidad del remitente, así como el envío de comunicaciones publicitaras o promocionales por medios electrónicos que no hubieren sido solicitados o autorizados expresamente por los destinatarios. Se exceptúan los casos en que exista una relación contractual previa, si el destinatario hubiere dado su consentimiento. Sin perjuicio, debe tener la posibilidad de oponerse, de forma sencilla y gratuita, así como de revocar en cualquier momento el consentimiento prestado[370].

Se prevé que los contratos celebrados por vía electrónica tendrán los mismos efectos que los contratos tradicionales cuando haya consentimiento y validez. Sirve como prueba el soporte electrónico en que conste el contrato celebrado, siendo admisible en juicio como prueba documental. Se establecen determinadas limitaciones, como ser contratos relativos al Derecho de familia, así como aquellos supuestos en que la norma exija la intervención de órganos jurisdiccionales, notarios, registradores de la propiedad y mercantiles o autoridades públicas, rigiéndose por la normativa específica[371].

Se disponen determinadas obligaciones a cumplir previo a la celebración del contrato electrónico, salvo si ninguno de los contratantes tiene la calidad de consumidor

[369] Artículo 18 de la Ley 34/2002.
[370] Artículos 19, 20, 21 y 22 de la Ley 34/2002.
[371] Artículos 23 y 24 de la Ley 34/2002.

o si se celebra exclusivamente por medio de correos electrónico o por medio de comunicación equivalente. Además de los requisitos básicos de información que se requieren en la normativa vigente, el prestador de servicios de la sociedad de la información debe poner a disposición del destinatario, de forma permanente, fácil y gratuita, información clara, comprensible e inequívoca sobre: (a) los trámites que debe seguir para celebrar el contrato, (b) si va a archivar el documento electrónico en el que se formalice el acuerdo y si será accesible, (c) los medios técnicos para identificar y corregir errores, y (d) la lengua de formalización el contrato. Se puede dar por cumplido lo anterior si el prestador incluye en su página dichas condiciones o si facilita de manera permanente, fácil, directa y exacta la dirección de Internet en que dicha información es puesta a disposición del destinatario[372].

Por el otro lado, también se establecen obligaciones a cumplir con posterioridad a la celebración del contrato, como ser confirmar la recepción de la aceptación, ya sea por acuse de recibo o por la confirmación por un medio equivalente al utilizado en el procedimiento de contratación. Sin embargo, no será necesaria la confirmación de la recepción cuando ambos contratantes así lo acuerden y ninguno sea considerado como consumidor, y cuando el contrato se haya celebrado por medio del intercambio de correos electrónico u otro medio similar[373].

Respecto al lugar de celebración del contrato, se entenderá que será el sitio donde el consumidor tenga su residencia habitual; en caso de que se celebre entre empresarios, se estará a lo pactado por las partes y, en su defecto, se presumirá celebrado donde el prestador del servicio esté establecido[374].

Se podrán someter los conflictos a arbitrajes conforme lo previsto en la ley de arbitraje y en la legislación de arbitraje y de defensa del consumidor, pudiendo hacer uso de medios electrónicos[375].

Interesa señalar que en lo que respecta al comercio electrónico, además de la LSSI, también se debe atender lo dispuesto por las leyes 56/2007 de Medidas de Impulso a la Sociedad de la Información y la 25/2013 de impulso a la factura electrónica.

[372] Artículos 26 y 27 de la Ley 34/2002.
[373] Artículo 28 de la Ley 34/2002.
[374] Artículo 29 de la Ley 34/2002.
[375] Artículo 32 de la Ley 34/2002.

Concluyendo, como enseña la Profesora Susana Checa: "*La mundialización de la economía ha traído como consecuencia la adopción de una estrategia global por parte de todos los agentes involucrados en las comunicaciones" (...)La regulación de todas las materias relacionadas con las tecnologías de la información queda rápidamente obsoleta ya que, en los últimos tiempos, vienen surgiendo necesidades nuevas y cambiantes en todos los ámbitos de la sociedad y, a su vez, se van comprobando lagunas en la normativa existente y tratan de subsanarse estos defectos con la promulgación de nuevas normas.*

Sin embargo, y a pesar de la enorme dificultad que sin duda alguna entraña dotar de regulación a los fenómenos relacionados con las nuevas tecnologías, el Derecho no puede quedar al margen de esta nueva realidad, dada la relevancia jurídica que han adquirido las operaciones realizadas a través de estos medios.

La adecuación e implementación de las TIC al ámbito del comercio electrónico supuso una serie de problemas normativos que, desde el primer momento, trataron de solventarse mediante la realización de planes cuatrienales.

Así, la Ley General de Telecomunicaciones (en adelante, LGT), incorporó una nueva disposición adicional (séptima) a la Ley de Comercio electrónico (en adelante, LSSI), indicando la necesidad de presentar un plan cuatrienal, que deberá "Potenciar decididamente las iniciativas de formación y educación en las tecnologías de la información para extender su uso; especialmente, en el ámbito de la educación, la cultura, la gestión de las empresas, el comercio electrónico y la sanidad"[9].

En definitiva, constantemente se está revisando y trabajando para impulsar y ajustar aquello que sea necesario para promover el desarrollo de los servicios de la sociedad de la información y el comercio electrónico.

(II.2.) Aspectos tributarios

La economía digital permite ofrecer servicios, productos y diversas soluciones en todo o en parte sobre las redes de telecomunicaciones, teniendo un impacto directo en toda la sociedad.

Puede plantearse como un canal más de comercialización que se suma al canal físico tradicional, pero también puede ser que se presente únicamente de forma online,

teniendo fácilmente alcance nacional e internacional, borrando fronteras, abriendo oportunidades y otorgando más posibilidades de elegir.

De esta forma, como señala CEPAL, se innova, atendiendo mejor el crecimiento económico, la inclusión social y la sostenibilidad ambiental, objetivos planteados en los ODS y la Agenda 2030 para el Desarrollo Sostenible[376].

En algunos casos los nuevos servicios y soluciones pueden competir con servicios tradicionales, innovando en la forma de otorgar la solución, mientras en otros casos pueden aparecen como soluciones y servicios completamente disruptivos.

La UE reconoce el auge que las empresas digitales han tenido, como ejemplo: las empresas de redes sociales, las plataformas colaborativas y los proveedores de contenidos en línea; mas entienden que la normativa fiscal no se concibió pensando en esta nueva realidad, ni en las empresas que operan a escala mundial, de forma virtual o que tienen escala o nula presencia física.

Por otra parte, como reconocen diversos autores, *¨las TIC permiten también a oferentes eludir regulaciones de distinto tipo, incluyendo obligaciones tributarias, lo que genera una situación de competencia desleal con aquellos que operan de la manera tradicional.¨*[377]

El 21 de setiembre de 2017 la Comisión Europea realizó la Comunicación Nº 547. Parte de la base de que las tecnologías digitales están transformando nuestro mundo, que tienen un gran impacto sobre los sistemas fiscales y que el MUD de la UE *"necesita un marco fiscal estable y moderno para que la economía digital estimule la innovación, acabe con la fragmentación del mercado y permita a todos los protagonistas aprovechar la nueva dinámica del mercado en condiciones justas y equilibradas. Resulta esencial garantizar la seguridad fiscal para la inversión empresarial y evitar que emerjan nuevas lagunas tributarias en el mercado único."*

Vale destacar que la fiscalidad es un elemento esencial para que los Estados tengan los medios necesarios para su adecuado desenvolvimiento y puedan cumplir eficazmente con sus fines. Es reflejo de las opciones de cada país en ámbitos esenciales del gasto público, como ser la educación, la sanidad y la pensiones, es muestra del

[376] https://www.cepal.org/fr/node/38413
[377] Economía Digital: Oportunidades y Desafíos: http://www.clapesuc.cl/investigaciones/doc-trabajo-no40-economia-digital-oportunidades-desafios/.

consumo privado y establece un marco financiero para la actividad empresarial y la protección del medio ambiente. Los gobiernos tienen libertad para establecer su legislación fiscal, mas deben respetar principios generales de la UE como es el de no discriminación y el de libre circulación en el mercado interior[378].

En este sentido, la UE supervisa las normas fiscales nacionales para garantizar que cumplan con las políticas europeas que: (i) fomentan el crecimiento económico, la creación de empleo, (ii) garantizan la libre circulación de mercancías, servicios y capitales, (iii) velan para que no se favorezca injustamente a las empresas de un país sobre sus competidores en otros países, y (iv) garantizan que los impuestos no discriminen a los consumidores, trabajadores o empresas de otros países de la UE[379].

Las decisiones fiscales de la UE necesitan de la unanimidad de todos los Estados miembros, a fin de tener en cuenta los intereses de todos los países. Si bien cada Estado miembro tiene libertad para decidir su gasto, en vistas de que puede afectar el crecimiento económico de los demás estados miembros, se trata de coordinar la política económica teniendo en cuenta las recomendaciones de la Comisión.

En esta línea en el caso del IVA e impuestos especiales sobre gasolina, tabaco y alcohol, se ha establecido marcos generales y tipos mínimos para evitar la distorsión de la competencia. En el caso del impuesto de sociedades y sobre la renta se trata de que se respete el principio de no discriminación y de libre circulación en el mercado único, para lo cual se necesita un marco coordinado.

Con el gran desarrollo del MUD, la Comisión Europea reconoce en su Comunicación[380], entre otras cosas: (i) dificultades para encontrar soluciones que permitan garantizar una fiscalidad justa y efectiva; (ii) que la actual normativa fiscal ha dejado de encajar, las empresas se sustentan en gran medida en activos intangibles difíciles de valorar; (iii) la necesidad del consenso internacional en cómo gravarlo, en tanto estamos en un mundo cada vez más globalizado y conectado digitalmente, en el que las actividades se desplazan cada vez más hacia el espacio digital; (iv) de no tratarse estos temas se favorecerá la elusión fiscal, los presupuestos públicos recibirán menos ingresos fiscales, la justicia social se verá afectada, desestabilizando la igualdad de

[378] Comisión Europea: ¨Fiscalidad¨. Publicado en https://publications.europa.eu/es/publication-detail/-/publication/b075f231-bd9b-4e10-b4a3-7f248360c5ae
[379] https://europa.eu/european-union/topics/taxation_es
[380] Comunicación de la Comisión Europea Nº 547 del 21 de setiembre de 2017.

condiciones para las empresas y afectando la competitividad de la UE, la justicia de la fiscalidad y la sostenibilidad; y (v) que la necesidad de la UE de un marco fiscal moderno para aprovechar las oportunidades del mundo digital, garantizando una fiscalidad justa, en tanto la igualdad de condiciones de competencia es requisito previo para que todas las empresas puedas innovar, desarrollarse y crecer, con el fin de apoyar la productividad, el empleo y la prosperidad.

En vista de lo anterior, se establece como reto reformar el marco fiscal internacional, pasando a disponer que el impuesto sobre sociedad debería gravar donde se genere el valor. El punto es que no siempre es evidente cuál es el valor, cómo se mide ni dónde se genera; por lo que se necesitaría reformar las normas fiscales sobre establecimiento permanente, la fijación de precios de transferencia y la atribución de beneficios aplicables a las tecnologías digitales.

Como se adelantó, los gobiernos nacionales tienen libertad para establecer su legislación fiscal, mas tienen que respetar determinados principios generales como es el de no discriminación y el de libre circulación en el mercado interior. La UE puede presentar propuestas si lo considera necesario para que el mercado funcione correctamente, en vista del principio de subsidiaridad y el de proporcionalidad[381].

Más allá de que se subraya la necesidad de alcanzar una solución internacional, considerando la complejidad de la temática y la gran variedad de cuestiones que deben abordarse, paralelamente a los debates internacionales, se proponen soluciones a escala de la UE.[382]

Reconociendo la nueva realidad y la importancia creciente de la economía digital, si bien se reconoce el trabajo que se ha venido realizando desde la OCDE, en el entendido de que no puede esperarse hasta el 2020, la UE presentó una solución provisional hasta que se alcance una solución global, buscando un marco fiscal uniforme y moderno para la economía digital.

Se presentaron dos propuestas diferentes para atender las actividades digitales[383]. Una provisional a corto plazo, que implica crear un Impuesto provisional sobre los

[381] https://publications.europa.eu/es/publication-detail/-/publication/b075f231-bd9b-4e10-b4a3-7f248360c5ae Consultado el 15 de enero de 2019.
[382] Comunicación de la Comisión al Parlamento Europeo y al Consejo Nº 146 del 21 de marzo de 2018. https://ec.europa.eu/transparency/regdoc/rep/1/2018/ES/COM-2018-146-F1-ES-MAIN-PART-1.PDF
[383] Ibídem.

Servicios Digitales a escala de la UE, y otra que requiere reformar las normas sobre el impuesto de sociedades a fin de que se declaren y graven los beneficios donde las empresas tengan una presencia digital significativa, ateniendo así los problemas de ¨dónde gravar¨ y ¨qué gravar¨ aunque no estén presentes físicamente.

La solución provisional reconoce que los Estados necesitan actuar sin tardanza, por lo que busca atender la necesidad de adoptar una solución provisional hasta que se acuerde una solución global. En esta línea, la Comisión propone un Impuesto provisional sobre los Servicios Digitales a escala de la UE, centrándose en actividades en que existe una gran diferencia entre el valor creado y la capacidad de los Estados para gravarlo. Según se indica, el Impuesto sobre los Servicios Digitales gravaría los ingresos procedentes de dos tipos principales de servicios digitales:

A los servicios consistentes en la inclusión de publicidad en interfaces digitales.

A las interfaces o mercados digitales intermediarios cuya finalidad principal es facilitar la interacción directa entre los usuarios (como las aplicaciones o sitios de venta entre particulares).

Por otra parte, a fin de no afectar a pequeñas o nuevas empresas se aplicarían umbrales, alcanzando a aquellas empresas que facturen más de 750 millones de euros en todo el mundo y más de 50 millones en la UE[384].

La propuesta dispone un impuesto del 3 % sobre la facturación por ciertos servicios digitales en los Estados miembros donde se localicen los usuarios, sería un impuesto sobre las ventas, buscando que no se traslade al cliente final[385].

Estaría destinado a tres actividades: el comercio electrónico (ejemplo servicios prestador por Amazon), las operaciones entre particulares a través de plataformas que ofrecen un servicio de red de consumo (ejemplo AirBnb) y la compra venta de datos de usuarios residentes en la Unión Europea[386].

---

384 http://www.lavanguardia.com/vida/20180428/443092967981/varios-paises-de-la-ue-bloquean-el-impuesto-a-los-gigantes-digitales.html

385 KPMG: Tributación directa de la Economía Digital: Iniciativas UE. Publicado en https://assets.kpmg.com/content/dam/kpmg/es/pdf/2018/04/tax-alert-tributacion-directa-econom%C3%ADa-digital-iniciativas-union-europea.pdf

386 https://www.larazon.es/economia/el-impuesto-digital-en-el-mundo-europa-marcha-a-dos-velocidades-EP18353654

Según ha trascendido en prensa, hay países a favor de la medida y otros que se presentan más prudentes apelando a tomar medidas más a largo plazo, trabajando a nivel internacional, promoviendo el consumo y no las haciendas estatales. La OCDE no es partidaria de este tipo de medidas.

En lo que respecta a la otra medida propuesta, que requiere reformar las normas sobre el IS a fin de que se declaren y graven los beneficios donde las empresas tengan una presencia digital significativa, ateniendo así los problemas de ¨dónde gravar¨ y ¨qué gravar¨ aunque no estén presentes físicamente. Se propone que las grandes empresas paguen impuestos donde tengan una presencia digital significativa.

El 21 de marzo de 2018 la Comisión Europea presentó una propuesta de Directiva por la que se establecen normas relativas a la fiscalidad de las empresas con una presencia digital significativa[387] (en adelante, ¨la propuesta¨).

La propuesta de Directiva amplía el concepto de establecimiento permanente, de manera que se incluya la presencia digital significativa.

En el artículo 4 de la propuesta se dispone que se considera que existe una ¨presencia digital significativa¨ en un Estado miembro, en un periodo impositivo, si la actividad ejercida a través de la misma consiste total o parcialmente en la prestación de servicios digitales a través de una interfaz digital – entendiendo por interfaz digital: cualquier tipo de programa informático, incluyendo sitios web y aplicaciones móviles- y se cumplen una o varias de las siguientes condiciones con respecto a la prestación de dichos servicios por parte de la entidad que ejerce esa actividad, junto con la prestación de tales servicios a través de una interfaz digital por cada una de las empresas asociadas de dicha entidad en términos agregados:

a) la proporción de los ingresos totales obtenidos en ese periodo impositivo y resultante de la prestación de los servicios digitales a usuarios situados en dicho Estado miembro durante el mismo periodo impositivo sea superior a 7.000.000 EUR;

b) el número de usuarios de uno o más de los servicios digitales que estén situados en ese Estado miembro en dicho periodo impositivo sea superior a 100.000;

[387] https://eur-lex.europa.eu/legal-content/ES/ALL/?uri=CELEX%3A52018PC0147

c) el número de contratos entre empresas para la prestación de tales servicios digitales que suscriban en ese periodo impositivo los usuarios situados en dicho Estado miembro sea superior a 3.000.

Con respecto al uso de los servicios digitales, se considerará que un usuario está situado en un Estado miembro, en un periodo impositivo, si el usuario utiliza un dispositivo en ese Estado miembro en ese periodo impositivo para acceder a la interfaz digital a través de la cual se prestan los servicios digitales. Para determinar que el dispositivo del usuario se utilizó en un Estado miembro, se atenderá a la dirección de Protocolo Internet (IP) del dispositivo o, si es más preciso, por cualquier otro método de geolocalización.

Los beneficios imputables a la presencia digital significativa o en relación con la misma en un Estado miembro solo serán imponibles en el marco del impuesto sobre sociedades de dicho Estado miembro. Serán los que la presencia digital debería haber percibido de haber sido una empresa separa e independiente que lleve a cabo actividades idénticas o similares, en condiciones idénticas o similares, en particular en sus tratos con otras partes de la empresa, teniendo en cuenta las funciones desempeñadas, los activos utilizados y los riesgos asumidos, a través de una interfaz digital[388]

En esta línea, la determinación de los beneficios imputables a la presencia digital significativa o en relación con la misma se basará en un análisis funcional. Para determinar las funciones de la presencia digital significativa y atribuirle la propiedad económica de los activos y los riesgos, se tendrán en cuenta las actividades significativas desde el punto de vista económico llevadas a cabo por dicha presencia a través de una interfaz digital. Con esta finalidad, las actividades emprendidas por la empresa a través de una interfaz digital relacionadas con datos o usuarios serán consideradas actividades significativas desde el punto de vista económico de la presencia digital significativa que asigna los riesgos y la propiedad económica de los activos a dicha presencia.

Asimismo, se tendrán debidamente en cuenta las actividades significativas desde el punto de vista económico realizadas por la presencia digital significativa que sean relevantes para el desarrollo, mejora, mantenimiento, protección y explotación de los

[388] Artículo 5 de la Propuesta de Directiva de la Comisión Europea por la que se establecen normas relativas a la fiscalidad de las empresas con una presencia digital significativa

activos intangibles de la empresa. Entre las actividades se encuentran: a) la recogida, el almacenamiento, el tratamiento, el análisis, el despliegue y la venta de datos a nivel de usuario; b) la recogida, el almacenamiento, el tratamiento y el despliegue de contenido generado por el usuario; c) la venta de espacio publicitario en línea; d) la puesta a disposición de contenidos creados por terceros en un mercado digital; y e) la prestación de cualesquiera servicios digitales no enumerados en las letras a) a d).

Vale señalar que los datos que puedan recopilarse de los usuarios a efectos de la aplicación de la propuesta de Directiva se limitan a los que indique el Estado miembro en el que esté situado el usuario, sin permitir la identificación del usuario[389], y que los Estados miembros adoptarán y publicarán, a más tardar el 31 de diciembre de 2019, las disposiciones legales, reglamentarias y administrativas necesarias para dar cumplimiento a lo establecido en la presente Directiva, debiendo aplicar dichas disposiciones a partir del 1 de enero de 2020 con respecto a los periodos impositivos que comiencen en esa fecha o después de esa fecha.[390]

Como señala KPMG, la clave del debate es alcanzar un consenso acerca del nexus territorial en la creación de valor de un negocio digital. El enfoque podría ser aplicado a todas las compañías, incluso de fuera de la UE, que tengan presencia digital significativa en la UE. Al respecto se reconoce que cuando se trate de países no miembros de la UE con convenios de doble imposición suscritos con Estados miembros, la medida podría ser contraria al convenio, y por tanto inaplicable. Al respecto destaca que la UE ha elaborado Recomendaciones para que los Estados miembros traten de adaptar su red de convenios bilaterales al nuevo modelo, actuando en un doble frente: cambiando la definición de establecimiento permanente e incorporando las nuevas reglas de atribución de beneficios para considerar la contribución de los usuarios y de los datos a la creación de valor[391].

[389] Artículo 7 de la Propuesta de Directiva de la Comisión Europea por la que se establecen normas relativas a la fiscalidad de las empresas con una presencia digital significativa

[390] Artículo 9 de la Propuesta de Directiva de la Comisión Europea por la que se establecen normas relativas a la fiscalidad de las empresas con una presencia digital significativa.

[391] KPMG: Tributación directa de la Economía Digital: Iniciativas UE. Publicado en https://assets.kpmg.com/content/dam/kpmg/es/pdf/2018/04/tax-alert-tributacion-directa-econom%C3%ADa-digital-iniciativas-union-europea.pdf

En lo que respecta a España, la Confederación Española de Organizaciones Empresariales[392] aprobó el ¨*Plan Digital 2020*¨[393] - ¨*La digitalización de la sociedad española*¨.

Reconoce entre los pilares básicos digitales: la educación, la innovación y el emprendimiento digital. En lo que respecta a los aspectos fiscales propone, entre otras cosas: i. Reducir las cargas administrativas y la presión fiscal soportada por el sector de las telecomunicaciones para equipararlo a la media de los países de la Unión Europea, "mismos servicios, mismas reglas". ii. Eliminar, como sujetos obligados, a los prestadores del servicio de comunicación electrónica que difunden canales de televisión, en lo referente a la inversión obligatoria para la financiación anticipada de la producción de obras europeas regulada en el apartado 3 del artículo 5 de la Ley 7/2010, de 31 de marzo, General de la Comunicación Audiovisual. iii. Apostar por una novedosa política fiscal centrada en los usuarios en lugar de los operadores, que consista en el establecimiento de incentivos fiscales a los usuarios por conectarse a las redes NGA (Ley Macrón en Francia). iv. Establecer incentivos fiscales para fomentar la banda ancha. v. Establecer exenciones fiscales para proyectos de inversión que permitan la transformación digital a las empresas. vi. Exonerar del pago de impuestos medioambientales a las actividades relacionadas con la prestación de servicios digitales, debido al impacto positivo que la prestación de estos servicios tiene para el medio ambiente. vii. Desarrollar medidas que promuevan la seguridad jurídica, como, por ejemplo, el que haya un corpus de norma va fiscal que se mantenga estable independientemente de los cambios de Gobierno. viii. Promover la simplificación administra. ix. Promover e incentivar la colaboración entre autoridades fiscales y empresas, de forma que sea más sencillo y rápido conocer la posición de la Administración y evitar riesgos futuros.

Por otra parte, en línea con las medidas comunicadas por la UE, a finales de abril de 2018 el Ministro de Economía de España indicó que el Gobierno presentaría cuanto antes el impuesto a las grandes empresas digitales en España, a fin de comenzar a recaudarlo en el 2019, que contribuya para pagar la subida de pensiones prevista, ¨aún

[392] Comisión de Sociedad Digital, Comisión de I+D+i, Comisión de Industria y Energía, Consejo de Turismo, Consejo de Transporte y la Logística, Comisión de Sanidad, Asuntos Sociales e Igualdad.

[393] http://contenidos.ceoe.es/CEOE/var/pool/pdf/publications_docs-file-334-plan-digital-2020-la-digitalizacion-de-la-sociedad-espanola.pdf

antes de que haya acuerdo a nivel europeo, en la línea de lo que han hecho otros países como Reino Unido, Italia, Francia o Alemania"[394].

Finalmente, el 15 de octubre de 2020 se aprobó la Ley 4/2020, del Impuesto sobre Determinados Servicios Digitales, que entrará en vigor el 16 de enero de 2021[395]. Como surge de la exposición de motivos, parte de la base de que la economía mundial ha adquirido carácter digital, que han surgido nuevas maneras de hacer negocios, que se basan en la capacidad de llevar actividades a distancia, en activos intangibles, en el valor de los datos y las contribuciones de los usuarios finales. Reconoce que las actuales normas fiscales no fueron concebidas para hacer frente a estos nuevos modelos, por lo que no resultan apropiadas, requiriendo ser revisadas.

Considerando lo expuesto, el nuevo impuesto sobre Determinados Servicios Digitales es de naturaleza indirecta, grava al 3% las prestaciones de determinados servicios digitales en donde exista intervención de usuarios situados en el territorio español. Lo anterior, es sin perjuicio de los regímenes forales de Concierto y Convenio económico en vigor, respectivamente, en los Territorios Históricos del País Vasco y en la Comunidad Foral de Navarra, así como de los tratados y convenios internacionales que hayan pasado a formar parte del ordenamiento interno, conforme a lo dispuesto en el artículo 96 de la Constitución Española.

El hecho imponible al impuesto es la prestación de los servicios digitales realizados en el territorio español, conforme a lo señalado anteriormente. Corresponde destacar que se considerarán a estos efectos "Servicios Digitales" exclusivamente a los servicios de publicidad en línea[396], los de intermediación en línea[397] y los de transmisión de datos[398].

---

[394] https://noticiasbancarias.com/economia-y-finanzas/30/04/2018/espana-propone-un-impuesto-digital-para-gravar-a-las-firmas-tecnologicas/157887.html Consultado el 15 de enero de 2020.

[395] Ley 4/2020: https://www.boe.es/buscar/act.php?id=BOE-A-2020-12355 Consultado el 8 de diciembre de 2020

[396] Artículo 4 (6) de la Ley 4/2020 se define "Servicios de publicidad en línea" como: "los consistentes en la inclusión en una interfaz digital, propia o de terceros, de publicidad dirigida a los usuarios de dicha interfaz. Cuando la entidad que incluya la publicidad no sea propietaria de la interfaz digital, se considerará proveedora del servicio de publicidad a dicha entidad, y no a la entidad propietaria de la interfaz."

[397] Artículo 4 (7) de la Ley 4/2020 se define "Servicios de intermediación en línea" como "los de puesta a disposición de los usuarios de una interfaz digital multifacética (que permita interactuar con distintos usuarios de forma concurrente) que facilite la

Son contribuyentes aquellas personas jurídicas que el importe neto de su cifra de negocios en el año natural anterior supere 750 millones de euros; y que el importe total de sus ingresos derivados de prestaciones de servicios digitales sujetas al impuesto, una vez aplicadas las reglas para determinar la base imponible, correspondientes al año natural anterior, supere 3 millones de euros[399].

El artículo 6 de la Ley 4/2020 excluye del impuesto: (a) las ventas de bienes o servicios contratados en línea a través del sitio web del proveedor de esos bienes o servicios, el proveedor no actúa en calidad de intermediario; (b) las entregas de bienes o la prestación de servicios subyacentes que tengan lugar entre los usuarios, en el marco de un servicio de intermediación en línea; (c) las prestaciones de servicios de intermediación en línea, cuando la única o principal finalidad de dichos servicios sea suministrar contenidos digitales a los usuarios o prestarles servicios de comunicación o servicios de pago; (d) las prestaciones de servicios financieros regulados por entidades financieras reguladas; (e) las prestaciones de servicios de transmisión de datos, cuando se realicen por entidades financieras reguladas; y (f) las prestaciones de servicios digitales cuando sean realizadas entre entidades que formen parte de un grupo con una participación, directa o indirecta, del 100 por cien.

Para el desarrollo normativo y la ejecución de la Ley, en la disposición final segunda se habilita al Gobierno a dictar cuantas disposiciones sean necesarias.

La norma es muy reciente y aún no ha entrado en vigor, por lo que se deberá atender en los próximos tiempos al desarrollo normativo, así como a la aplicación de la misma.

---

realización de entregas de bienes o prestaciones de servicios subyacentes directamente entre los usuarios, o que les permita localizar a otros usuarios e interactuar con ellos."

[398] Artículo 4 (8) de la Ley 4/2020 se define "Servicios de transmisión de datos" como "los de transmisión con contraprestación, incluidas la venta o cesión, de aquellos recopilados acerca de los usuarios, que hayan sido generados por actividades desarrolladas por estos últimos en las interfaces digitales".

[399] Artículo 8 de la Ley 4/2020.

(II.3.) Pagos y dinero electrónicos, monedas digitales y financiamiento colectivo

(II.3.A.)Pagos electrónicos

El 23 de noviembre de 2018 se aprobó el Real Decreto 19/2018 de servicios de pago y otras medidas urgentes en materia financiera. Parte de la base de que un mercado de servicios de pago adecuado es básico para construir el MUD de la UE, siendo esencial adaptar la regulación a los cambios tecnológicos que permitan a los usuarios disponer de nuevos servicios de pago, en entornos más seguros y fiables.

Como antecedentes se cuenta con la Ley 16/2009 de servicios de pago, por medio de la cual se transpone la Directiva 2007/64/CE del Parlamento Europeo y del Consejo sobre servicios de pago en el mercado interior, facilitando entre otras cosas, la aplicación de los instrumentos de pago en euros dentro de la zona única de pagos; la cual se adapta a fin de reflejar los nuevos servicios de pago, el impacto de internet y de los nuevos dispositivos, otorgando un ecosistema más seguro.

Por otra parte, atiende la urgencia de adaptar el mercado financiero de España a la PSD2, en tanto: (i) el plazo estaba vencido y la Comisión Europea remitió carta de emplazamiento por infracción por falta de transposición; (ii) la incertidumbre regulatoria generaba perjuicios a las entidades de crédito y de pago, así como a los usuarios; y (iii) se estaba afectando la competitividad, limitando la capacidad de atraer al mercado español nuevos proveedores de servicios de pago.

Se quiere adaptar la regulación a los cambios tecnológicos, generando entornos más seguros y fiables, y permitiendo que los usuarios dispongan de nuevos servicios de pago y de nuevos agentes más fiables. En este sentido, regula tres aspectos principales: (i) los servicios a prestar, (ii) la transparencia frente al usuario, y (iii) las obligaciones de las partes intervinientes.

Partiendo de esta base, genera cambios en el mercado de valores[400], en el mercado bancario[401] y en el mercado de servicios de pago.

[400] Como surge de la Exposición de Motivos: "La disposición final novena modifica el texto refundido de la Ley del Mercado de Valores, aprobado por el Real Decreto Legislativo 4/2015, de 23 de octubre. Los objetivos que se persiguen con esta modificación son los siguientes: en primer lugar, se lleva a cabo una adecuación formal y técnica de algunas de sus disposiciones. En segundo lugar, se adapta la norma a distintos reglamentos europeos recientes cuya entrada en vigor y aplicación efectiva ya se ha producido". Específicamente: (i) el Reglamento (UE) Nº

En lo que respecta al tercer punto, se consideran los servicios de pagos que se presten con carácter profesional, "*incluyendo la forma en que se prestan dichos servicios, el régimen jurídico de las entidades de pago, el régimen de transparencia e información aplicable a los servicios de pago, así como los derechos y obligaciones respectivas tanto de los usuarios de los servicios de pago como de los proveedores de los mismos.*[402] ,,

Los servicios de pago que se regulan son aquellos que permiten:

- ingresar efectivo en una cuenta de pago y su gestión.
- retirar efectivo de una cuenta de pago y su gestión.
- Ejecutar operaciones de pago, a través de una cuenta de pago en el proveedor de servicios de pago del usuario u otro proveedor de servicios de

---

2016/2011 del Parlamento Europeo y del Consejo de 8 de junio de 2016 sobre os índices utilizados como referencia en los instrumentos financieros y en los contratos financieros o para medir la rentabilidad de los fondos de inversión, (ii) el Reglamento (UE) Nº 596/2014 del Parlamento Europeo de y del Consejo de 16 de abril de 2014 sobre el abuso de mercado, (iii) el Reglamento (UE) n.º 1286/2014 del Parlamento Europeo y del Consejo de 26 de noviembre de 2014 sobre los documentos de datos fundamentales relativos a los productos de inversión minorista vinculados y los productos de inversión basados en seguros, y (iv) el Reglamento (UE) n.º 2015/2365 del Parlamento Europeo y del Consejo de 25 de noviembre de 2015 sobre sobre transparencia de las operaciones de financiación de valores y de reutilización. Además se completa la transposición de dos Directivas: Directiva de Ejecución (UE) 2015/2392 de la Comisión de 17 de diciembre de 2015, sobre la comunicación de posibles infracciones o infracciones reales del Reglamento (UE) n.º 596/2014; y la Directiva 2013/36/UE del Parlamento Europeo y del Consejo de 26 de junio de 2013 sobre el acceso a la actividad de las entidades de crédito y a la supervisión prudencial de las entidades de crédito y las empresas de inversión.

[401] "La disposición final sexta modifica el régimen sancionador de la Ley 10/2014, de 26 de junio, de ordenación, supervisión y solvencia de entidades de crédito, para adaptarla a la actividad de prestación de servicios de pago y completar la adaptación de la normativa a la Directiva 2013/36/UE del Parlamento Europeo y del Consejo, de 26 de junio de 2013, relativa al acceso a la actividad de las entidades de crédito y a la supervisión prudencial de las entidades de crédito y las empresas de inversión, por la que se modifica la Directiva 2002/87/CE y se derogan las Directivas 2006/48/CE y 2006/49/CE y homologar el régimen sancionador español al de otros Estados Miembros y el Banco Central Europeo. Destaca especialmente la habilitación de un canal adecuado para que toda persona que disponga de conocimiento o sospecha fundada de incumplimiento de las obligaciones en materia de supervisión prudencial de entidades de crédito previstas en dicha ley y su normativa de desarrollo tenga la posibilidad y el derecho a comunicarlo al Banco de España con las debidas garantías (también conocido como *whistleblowing*)." Asimismo, "La disposición final séptima modifica la Ley 5/2015, de 27 de abril, de fomento de la financiación empresarial, para atribuir al Banco de España la autorización de los establecimientos financieros de crédito híbridos. En la medida que los Establecimientos Financieros de Crédito híbridos prestan servicios de pago, esta modificación es coherente con el hecho de que se le atribuyan al Banco de España las competencias en autorización de las entidades de pago en este real decreto-ley."

[402] Artículo 1 del Real Decreto

pago. Incluye: adeudos domiciliados[403], operaciones de pago[404] por medio de tarjetas de pago o dispositivos similares, y transferencias[405].

- Ejecutar operaciones de pago en el caso que los fondos estén cubiertos por una línea de crédito abierta para un usuario de servicios de pago. Incluye: adeudos domiciliarios, operaciones de pago por medio de tarjetas de pago o dispositivos similares, y transferencias.
- Emitir instrumentos de pago[406] o la adquisición de operaciones de pago.
- Enviar dinero.
- Servicios de iniciación de pagos[407].
- Servicios de información sobre cuentas[408].

Los dos últimos son tipos nuevos de servicios, que hasta el momento no habían sido objeto de regulación en España, implica el acceso de terceros a las cuentas de los usuarios de servicios de pago, dando más seguridad y protección.

El servicio de iniciación de pagos da la seguridad de que el pago se ha iniciado, incentivando la entrega del bien o la prestación del servicio sin dilación desde el

[403] El artículo 3.1. del Real Decreto 19/2018 define "adeudo domiciliado" como: *"servicio de pago destinado a efectuar un cargo en la cuenta de pago del ordenante, en el que la operación de pago es iniciada por el beneficiario sobre la base del consentimiento dado por el ordenante al beneficiario, al proveedor de servicios de pago del beneficiario o al proveedor de servicios de pago del propio ordenante"*

[404] El artículo 3.26. del Real Decreto 19/2018 define "Operación de pago" como *"una acción, iniciada por el ordenante o por cuenta de éste, o por el beneficiario, consistente en ingresar, transferir o retirar fondos, con independencia de cualesquiera obligaciones subyacentes entre el ordenante y el beneficiario."*

[405] El artículo 3.45. del Real Decreto 19/2018 define "Transferencia": "*servicio de pago destinado a efectuar un abono en una cuenta de pago de un beneficiario mediante una operación de pago o una serie de operaciones de pago con cargo a una cuenta de pago de un ordenante por el proveedor de servicios de pago que mantiene la cuenta de pago del ordenante, y prestado sobre la base de las instrucciones dadas por el ordenante."*

[406] El artículo 3.23 del Real Decreto 19/2018 define al "Instrumento de pago" como *"cualquier dispositivo personalizado o conjunto de procedimientos acordados entre el usuario de servicios de pago y el proveedor de servicios de pago y utilizados para iniciar una orden de pago."*

[407] El artículo 3.39 del Real Decreto 19/2018 lo define como el *"servicio que permite iniciar una orden de pago, a petición del usuario del servicio de pago, respecto de una cuenta de pago abierta con otro proveedor de servicios de pago."*

[408] El artículo 3.28 del Real Decreto 9/2018 lo define como el *"servicio en línea cuya finalidad consiste en facilitar información agregada sobre una o varias cuentas de pago de las que es titular el usuario del servicio de pago bien en otro proveedor de servicios de pago, bien en varios proveedores de servicios de pago."*

momento en que se da la orden de pago; y el servicio de información sobre cuentas, proporciona información agregada en línea, lo que permite tener en todo momento información global e inmediata de su situación financiera. Interesa destacar que los usuarios de servicios de pago pueden acceder a la información sobre cuentas, salvo que no se pueda acceder en línea, no requiriendo para ello la existencia de una relación contractual.

El artículo 5 del Real Decreto 19/2018 prevé que solo podrán prestar los servicios de pago, con carácter profesional, seis categorías de proveedores:

"a) Las entidades de crédito a que se refiere el artículo 1 de la Ley 10/2014, de 26 de junio, de ordenación, supervisión y solvencia de entidades de crédito, incluidas las sucursales en España de entidades de crédito extranjeras, tanto si las administraciones centrales de esas sucursales están ubicadas en el interior de la Unión Europea como si lo están fuera de ella.

b) Las entidades de dinero electrónico a que se refiere el artículo 2.1 b) de la Ley 21/2011, de 26 de julio, de dinero electrónico, incluidas las sucursales en España de entidades de dinero electrónico extranjeras, tanto si las administraciones centrales de esas sucursales están ubicadas en el interior de la Unión Europea como si lo están fuera de ella, en la medida en que los servicios de pago prestados por las sucursales estén vinculados a la emisión de dinero electrónico.

c) Las entidades de pago, reguladas en el título I[409] *y las entidades acogidas a lo establecido en los artículos 14*[410] *y 15*[411]*.*

[409] El Título I del Real Decreto 19/2018 establece el Régimen Jurídico de las entidades de Pago. Reserva la denominación "entidad de pago" (EP) a una persona jurídica a la cual se haya otorgado autorización para prestar y ejecutar servicios de pago en toda la Unión Europea, en los términos previstos en el artículo 11 del Real Decreto. Interesa destacar que las EP no pueden captar depósitos u otros fondos reembolsables del público ni emitir dinero electrónico. Las autorizaciones para poder operar pueden ser para algunos o para todos los servicios de pago. Es competencia del Banco de España, previo informe del Servicio ejecutivo de la Comisión de prevención del blanqueo de capitales e infracciones monetarias en los aspectos de su competencia, autorizar la creación de las EP. El régimen de autorización apunta a mantener el mayor nivel posible de competencia en la prestación de los servicios de pago; y se rige por los principios de celeridad, antiformalismo y economía procedimental.

[410] El artículo 14 del Real Decreto prevé el régimen de exención de las entidades de pago, no obstante tener que inscribirse, previa verificación por el Banco de España de determinados requisitos.

[411] El artículo 15 prevé el régimen de las EP del servicio de información sobre cuentas.

d) La Sociedad Estatal de Correos y Telégrafos, S.A., respecto de los servicios de pago para cuya prestación se encuentra facultada en virtud de su normativa específica."

Además, a estos efectos también se considera como proveedores de servicios de pago, cuando no actúen en su condición de autoridades públicas: al Banco Central Europeo, el Banco de España y los demás bancos centrales nacionales, y a la Administración General del Estado, las Comunidades Autónomas y las Entidades Locales.

Interesa destacar que las normas para acceder a los sistemas de pago deben ser objetivas, no discriminatorias, proporcionales y no pueden dificultar el acceso más de lo necesario para prevenir riesgos específicos, como pueden ser: liquidación, riesgos operativos, de explotación y garantizar la estabilidad operativa y financiera. No pueden requerir: (i) normas que limiten la participación en otros sistemas de pago, (ii) normas que discriminen entre los diversos proveedores de servicios de pago, ni (iii) restricciones basadas en estatutos institucionales[412].

En esta línea, se prevé que las entidades de pago deben tener acceso amplio a los servicios de cuentas de pago de las entidades de crédito de forma objetiva, no discriminatoria y proporcionada, permitiendo que las entidades de pago presten servicios de pago sin obstáculos y con eficiencia[413].

Por otra parte, dentro de las actividades que realizan las personas jurídicas que prestan los servicios de pago, las entidades de pago (EP) también están habilitadas para realizar las siguientes actividades: (i) prestar servicios operativos o auxiliares estrechamente relacionados, (ii) la gestión de sistemas de pago, y (iii) otras actividades empresariales, pudiendo exigírseles en caso de que dichas actividades pudieran perjudicar la solidez financiera de la entidad, que deban constituir una entidad separada[414].

Las EP deben proteger los fondos recibidos de los usuarios de los servicios de pago, sujetándose a uno de los siguientes dos procedimientos: (1) los fondos no pueden confundirse con los fondos de persona que no sean usuarios de servicios de pago en cuyo nombre se dispone de los fondos y, en caso de que todavía estén en posesión de la

[412] Artículo 8 del Real Decreto 19/2018.
[413] Artículo 9 del Real Decreto 19/2018.
[414] Artículo 20 del Real Decreto 19/2018.

entidad de pago y aún no se hayan entregado al beneficiario o transferido a otro proveedor de servicios de pago al final del día hábil siguiente al día en que se recibieron los fondos, se depositarán en una cuenta separada en una entidad de crédito o se invertirán en activos seguros, líquidos y de bajo riesgo en los términos que se establezcan reglamentariamente. (2) En caso de que vayan a confundirse, los fondos deben estar cubiertos por una póliza de seguro u otra garantía comparable[415], por una cantidad equivalente, que se efectivizará en caso de que la entidad de pago no pueda hacer frente a sus obligaciones financieras[416].

Asimismo, se atiende especialmente la seguridad de los servicios, previendo diversas medidas, los fraudes informáticas y atribuyendo distintas responsabilidades.

Los proveedores de servicios de pago deben cumplir con determinadas normas para acceder a la información sobre las cuentas de pago, así como respecto al uso de la información. En este sentido, los proveedores del servicio de información sobre cuentas deben: (a) requerir consentimiento explícito del usuario; (b) garantizar que las credenciales de seguridad personalizadas del usuario no sean accesibles a terceros y que cuando las transmita lo haga a través de canales seguros y eficientes; (c) exigir que el usuario se identifique en cada comunicación y que se comunique de manera segura[417]; (d) restringir el acceso a la información de las cuentas de pago designadas por el usuario y a las operaciones de pago que correspondan; (e) no solicitar datos de pago sensibles vinculados a las cuentas de pago; (f) no utilizar, almacenar o acceder a datos, para fines distintos de los expresamente solicitados, conforme con las normas sobre protección de datos.

En esta línea, los proveedores del servicio de pago deben tratar las peticiones de datos sin discriminación alguna, salvo razones objetivas.

Para prevenir los fraudes y cubrir debidamente la seguridad es esencial trabajar en toda la cadena. En este sentido, se prevén obligaciones para los usuarios de los servicios y para los proveedores de servicios, pruebas de autenticación y de ejecución de las operaciones de pago, y diversas responsabilidades.

---

[415] "De una compañía de seguros o de una entidad de crédito que no pertenezcan al mismo grupo que la propia entidad de pago". (Artículo 21.b del Real Decreto)

[416] Artículo 21 del Real Decreto 19/2018.

[417] De conformidad con lo previsto en el Reglamento Delegado 2018/389 y a los criterios que determine el Banco de España.

En relación a las obligaciones, se establecen específicas para los usuarios y otras para los proveedores de servicios de pago en relación con los instrumentos de pago.

Los usuarios deben[418]: (i) utilizar los instrumentos como establecen las condiciones que regulan su emisión y utilización, las cuales deben ser objetivas, no discriminatorias y proporcionadas; (ii) tomar todas las medidas razonables a fin de proteger sus credenciales de seguridad personalizadas; y (iii) notificar sin demoras en cuanto tenga conocimiento al proveedor de servicios o a la entidad que este designe, en caso de extravío, sustracción o apropiación indebida del instrumento de pago o de su utilización no autorizada[419].

Los proveedores deben: (i) asegurar que las credenciales de seguridad solo sean accesibles para el usuario de servicios de pago facultado para utilizar dicho instrumento; (ii) abstenerse de enviar instrumentos de pago que no hayan sido solicitados, salvo en caso de que deba sustituirse el instrumento ya entregado al usuario[420]; (iii) garantizar medios gratuitos y adecuados para que el usuario pueda notificar de forma inmediata tras tomar conocimiento del extravío, sustracción o apropiación indebida del instrumento de pago o su utilización no autorizada, así como para solicitar el desbloqueo del instrumento de pago o la sustitución de otro nuevo una vez que haya cesado el motivo del bloqueo; (iv) facilitar al usuario poder demostrar que ha realizado las comunicaciones que correspondan durante los 18 meses siguientes a la realización; (v) impedir la utilización del instrumento de pago cuando se haya denunciado su extravío, sustracción o uso no autorizado; (vi) soportar los riesgos por enviar instrumentos de pago al usuario de servicio de pago o del envío de cualquier elemento de seguridad personalizado.

En caso de que el usuario de servicios de pago niegue haber autorizado una determinada operación ya ejecutada o indique que se realizó de forma incorrecta, será obligación del proveedor mostrar que la operación fue autenticada, realizada con

[418] Artículo 41 del Real Decreto Nº 19/2018.

[419] El usuario de servicio de pago tendrá la rectificación de una operación de pago no autorizada o ejecutada incorrectamente, por parte del proveedor de servicios de pago, únicamente si el usuario se lo comunica sin demora injustificada, en cuanto tenga conocimiento, y dentro de un plazo máximo de trece meses contados desde la fecha del adeudo (Artículo 43.1 del Real Decreto 19/2018).

[420] La sustitución puede ser por la incorporación de nuevas funcionalidades, aunque no hayan sido expresamente solicitadas por el usuario, si en el contrato se hubiera previsto la posibilidad y sea gratUITo para el cliente.

exactitud y contabilizada, así como que no fue afectada por un fallo técnico u otra deficiencia del servicio. Le corresponde al proveedor del servicio conservar la documentación y los registros que acrediten el cumplimiento de sus obligaciones, debiendo facilitarlas al usuario en caso de que sean requeridas, por lo menos por el plazo de 6 años. Sin perjuicio, conservará la documentación relativa a la relación jurídica que le une con cada usuario de servicio por lo menos por el período de prescripción de los derechos y obligaciones contractuales.

En caso de que se ejecute una operación de pago no autorizada, se devolverá al usuario el importe de la operación no autorizada de inmediato, a más tardar al final del día hábil siguiente a aquel en el que haya observado o notificado la operación, salvo cuando haya motivos razonables para sospechar que hubo fraude, lo cual se comunicará al Banco de España. Asimismo, en caso de que el responsable de la operación de pago no autorizada sea el proveedor de servicios de iniciación de pagos, éste deberá resarcir de inmediato al proveedor de servicios de pago gestor de cuenta por las pérdidas sufridas o las sumas abonadas para efectuar la devolución al ordenante, incluido el importe de la operación de pago no autorizada. Se prevé además, que podrán determinarse otras indemnizaciones económicas, según corresponda.

Por otra parte, en relación a la responsabilidad del cliente en caso de operaciones de pago no autorizadas, se prevén dos supuestos: (1) que deberá soportar hasta un máximo de 50 euros por las pérdidas que deriven de la utilización de un instrumento de pago extraviado, sustraído o apropiado indebidamente por un tercero[421]; y (2) que deberá soportar todas las pérdidas por operaciones de pago no autorizadas, si el ordenante actuó de forma fraudulenta o incumplió, deliberadamente o por negligencia grave, con una o varias de sus obligaciones previstas en el artículo 41 del Real Decreto Nº 19/2018.

En definitiva, el Real Decreto 19/2018 entró en vigor el 25 de noviembre de 2018, sin perjuicio de que algunas de sus disposiciones entraron en vigencia el 24 de febrero de 2019, y abarca los servicios de pago prestados dentro de España. Entre las particularidades se destaca el hecho de que dispone obligaciones y responsabilidades

[421] Excepto que: *"a) al ordenante no le resultara posible detectar la pérdida, la sustracción o la apropiación indebida de un instrumento de pago antes de un pago, salvo cuando el propio ordenante haya actuado fraudulentamente, o b) la pérdida se debiera a la acción o inacción de empleados o de cualquier agente, sucursal o entidad de un proveedor de servicios de pago al que se hayan externalizado actividades"* (artículo 46 del Real Decreto Nº 19/2018)

tanto para los usuarios, como para los proveedores de servicios, lo cual es esencial para prever los fraudes y asegurar la prestación de los servicios.

(II.3.B) Dinero electrónico

Interesa señalar que los primeros instrumentos de prepago electrónico dieron lugar a la Directiva 2000/46/CE[422], de 18 de setiembre de 2000, sobre el acceso a la actividad de las entidades de dinero electrónico y su ejercicio, así como la supervisión de dichas entidades. Dicha Directiva se incorporó al ordenamiento jurídico español a través del artículo 21 de la Ley 44/2002, de 22 de noviembre, de medidas de reforma del sistema financiero y el Real Decreto 322/2008, de 29 de febrero, sobre el régimen jurídico de las entidades de dinero electrónico.

La evolución y el desarrollo ha sido constate, lo cual fue acompañado por la regulación, la cual se fue actualizando, en tanto se vio la necesidad de mejorar la efectividad práctica para contribuir al desarrollo del mercado.

En esta línea, entre las principales necesidades se destacó la importancia de modificar características del dinero electrónico y de la actividad de emisión del mismo, para aumentar la seguridad jurídica en el desarrollo de la actividad y para que el marco jurídico sea consistente con el régimen jurídico de los servicios de pago.

Considerando lo expuesto se aprobó la Ley Nº 21/2011, de 26 de julio, con tres objetivos fundamentales: (1) aumentar la precisión del régimen jurídico aplicable a la emisión de dinero electrónico, lo cual da más seguridad jurídica y por ende se facilita el acceso a la actividad de emisión de dinero electrónico y se estimula la competencia. (2) Buscar un régimen más proporcionado, por lo que se eliminan requerimientos que por resultar demasiado onerosos para las entidades son inadecuados en relación con los riesgos que su actividad puede potencialmente generar. (3) Garantizar la consistencia entre el nuevo régimen jurídico de las entidades de pago y el aplicable a las entidades de dinero electrónico.

La Ley Nº 21/2011 regula el dinero electrónico y lo define como *"todo valor monetario almacenado por medios electrónicos o magnéticos que represente un crédito sobre el emisor, que se emita al recibo de fondos con el propósito de efectuar*

[422] La Directiva 2009/110/CE, de 16 de septiembre de 2009, sobre el acceso a la actividad de las entidades de dinero electrónico y su ejercicio, así como sobre la supervisión prudencial de dichas entidades, modificó las Directivas 2005/60/CE y 2006/48/CE y derogó la Directiva 2000/46/CE.

operaciones de pago (…), y que sea aceptado por una persona física o jurídica distinta del emisor de dinero electrónico"[423].

Interesa señalar que el Real Decreto Nº 19/2018 define "fondos" como "*los billetes y monedas, dinero bancario o dinero electrónico, entendido como todo valor monetario almacenado por medios electrónicos o magnéticos que represente un crédito sobre el emisor, que se emita al recibo de fondos con el propósito de efectuar operaciones de pago y que sea aceptado por una persona física o jurídica distinta del emisor de dinero electrónico.*[424]*",* y que "Operación de pago" es "*una acción, iniciada por el ordenante o por el beneficiario, consistente en situar, transferir o retirar fondos, con independencia de cualesquiera obligaciones subyacentes entre ambos*[425]*".*

La emisión de dinero electrónico está reservada a determinadas categorías de emisores, estando prohibido que toda persona física o jurídica distinta lo emita[426]. Se busca fomentar la competencia y abrir la emisión de dinero electrónico a instituciones distintas de las bancarias, por lo que se crean las entidades de dinero electrónico (EDE).

Las EDE son aquellas personas jurídicas, distintas a las entidades de crédito, que se les haya autorizado a emitir dinero electrónico. Son supervisadas por el Banco de España, quien controla e inspecciona las EDE, así como su inscripción en el Registro Especial de Entidades de Dinero Electrónico.

Las disposiciones transitorias primera a novena del Real Decreto Nº 19/2018 buscan adaptar las entidades de pago y a las entidades de dinero electrónico a la nueva regulación. Asimismo, la disposición final quinta modifica la normativa sobre las entidades de dinero electrónico conforme a la PSD2.

---

[423] Artículo 1.2 de la Ley 21/2011.
[424] Artículo 3.19 del Real Decreto Nº 19/2018.
[425] Artículo 2.5 de la Ley 16/2009.
[426] El artículo 2.1 de la Ley 21/2011 prevé la reserva de la actividad de emitir dinero electrónico y dispone que *"Podrán emitir dinero electrónico las siguientes categorías de emisores de dinero electrónico: a) Las entidades de crédito, a que se refiere el artículo 1.2 del Real Decreto Legislativo 1298/1986, de 28 de junio, sobre adaptación del Derecho vigente en materia de entidades de crédito al de las Comunidades Europeas, y cualquier sucursal en España de una entidad de crédito cuya matriz esté domiciliada o autorizada fuera de la Unión Europea. b) Las entidades de dinero electrónico autorizadas conforme al artículo 4 de esta Ley y cualquier sucursal en España de una entidad de dinero electrónico cuya matriz esté domiciliada o autorizada fuera de la Unión Europea. c) La Sociedad Estatal de Correos y Telégrafos, S.A., respecto de las actividades de emisión de dinero electrónico a que se encuentre facultada en virtud de su normativa específica. d) El Banco de España, cuando no actúe en su condición de autoridad monetaria. e) La Administración General del Estado, las Comunidades Autónomas y las Entidades Locales, cuando actúen en su condición de autoridades públicas."*

Interesa destacar que no debe confundirse el dinero electrónico con las monedas digitales o criptomonedas.

(II.3.C) Monedas digitales

Las criptomonedas no tienen una regulación específica en España, no obstante, la Agencia Tributaria en su Plan de Control Tributario de 2018 indicó que vigilaría el empleo de las criptomonedas como método de pago, y hay consultas vinculantes[427] sobre la materia debiendo realizarse declaraciones según las transacciones que se realicen[428].

Como informa Group BTC *"Los impuestos sujetos a tributación según el tipo de transacción son el relativo a los beneficios por la compraventa e intercambio de criptomonedas y el impuesto sobre el patrimonio. Los beneficios y pérdidas obtenidos en las operaciones de compra y venta de estos activos tributarán como ganancia o pérdida patrimonial en el IRPF. Se deben utilizar los mismos criterios de valoración que en el caso de las operaciones con acciones." (...) "la minería de criptomonedas" tiene la "obligación de darse de alta en el impuesto sobre actividades económicas asimilando las actividades relacionadas con criptomonedas a las propias de los servicios financieros"*[429].

Además desde una sentencia del Tribunal de Justicia de la Unión Europea (TJUE), de fecha 22 de octubre de 2015 (asunto C-264/14), las reconoce como una divisa no tradicional, que es un medio de pago y además puede constituir operaciones financieras.

Por otra parte, interesa hacer mención a una sentencia de la Sala de lo Penal del Tribunal Supremo de España, Nº 998/2018 del 20 de junio de 2019, en un caso vinculado con una estafa realizada con bitcoins, por una empresa de trading. El Tribunal señaló que Bitcoin es: (i) *"una unidad de cuenta de la red del mismo nombre. A partir de un libro de cuentas público y distribuido, donde se almacenan todas las transacciones de manera permanente en una base de datos denominada Blockchain, se*

---

[427] DIRECCION GENERAL DE TRIBUTOS. URL: https://nevtrace.com/wp-content/uploads/2017/08/V1028-15.pdf Consultado el 20 de julio de 2019.

[428] ALGORITMO LEGAL. URL: https://www.algoritmolegal.com/tecnologias-disruptivas/regulacion-legal-del-bitcoin-y-de-otras-criptomonedas-en-espana/ Consultado el 20 de julio de 2019.

[429] GROUP BTC en "Regulación y legislación de las criptomonedas", URL: https://www.groupbtc.com/es/articulo/regulacion-y-legislacion-de-criptomonedas Consultado el 20 de julio de 2019.

crearon 21 millones de estas unidades, que se comercializan de manera divisible a través de una red informática verificada". (ii) "un activo patrimonial inmaterial, en forma de unidad de cuenta definida mediante la tecnología informática y criptográfica denominada bitcoin, cuyo valor es el que cada unidad de cuenta o su porción alcance por el concierto de la oferta y la demanda en la venta que de estas unidades se realiza a través de las plataformas de trading Bitcoin" (iii) "un activo inmaterial de contraprestación o de intercambio en cualquier transacción bilateral en la que los contratantes lo acepten, pero en modo alguno es dinero". En el caso se planteó la restitución y el Tribunal señaló que *"por más que la prueba justificara que el contrato de inversión se hubiera hecho entregando los recurrentes bitcoins y no los euros que transfirieron al acusado, el Tribunal de instancia no puede acordar la restitución de los bitcoins"*. Finalmente, en relación a la forma de reparar el daño e indemnizar los perjuicios, falló que debía hacerse "*retornado a los perjudicados el importe de la aportación dineraria realizada (daño), con un incremento como perjuicio que concreta en la rentabilidad que hubiera ofrecido el precio de las unidades bitcoin entre el momento de la inversión y la fecha del vencimiento de sus respectivos contratos*."

Uno de los aspectos que más preocupa a las autoridades es el hecho de que las monedas digitales se puedan utilizar para lavar activos o financiar el terrorismo. En esta línea, la Directiva (UE) 2018/843/UE del Parlamento Europeo y del Consejo de 20 de mayo de 2018, modificó la Directiva 2015/840 relativa a la prevención de la utilización del sistema financiero para el blanqueo de capitales o la financiación del terrorismo, debiendo los Estados miembros transponerla antes del 10 de enero de 2020. Lo que más se destacó de dicha Directiva es que definió las monedas virtuales como: "*representación digital de valor no emitida ni garantizada por un banco central ni por una autoridad pública, no necesariamente asociada a una moneda establecida legalmente, que no posee el estatuto jurídico de moneda o dinero, pero aceptada por personas físicas o jurídicas como medio de cambio y que puede transferirse, almacenarse y negociarse por medios electrónicos",* y que incluyó entre los sujetos obligados a los proveedores de servicios de cambio de moneda virtual a moneda fiduciaria y a los proveedores de servicios de custodia de monederos electrónicos.

Cabe señalar que las monedas digitales son un fenómeno relativamente reciente, en crecimiento constante[430]. En este sentido, según un estudio de ING de junio de 2018: *"el 32% de los españoles espera comprar criptomonedas en el futuro", "más de un tercio (38%) afirma que las criptomonedas son el futuro de los pagos online y un 37% que son el futuro de la inversión"*[431].

Interesa destacar que como surge del Boletín Oficial de las Cortes Generales, Senado, el 12 de febrero de 2018, el Pleno del Senado, en su sesión número 30, del 7 de febrero de 2018: *"El Senado insta al Gobierno a que traslade en los ámbitos y foros internacionales pertinentes (especialmente en el G20 que se celebrará en marzo del presente año y en los foros y organizaciones internacionales a los que acudan los ministros de finanzas) la necesidad de estudiar y evaluar la adopción de una regulación supranacional que permita generar confianza y fiabilidad en nuestros mercados, advierta a los inversores y usuarios de criptomonedas de sus riesgos y regule las entidades que lo comercialicen."*

Además señala aquellos aspectos que entienden que deben estar en una eventual regulación de la materia. Menciona los siguiente:

"1. El componente especulativo de las criptomonedas dificulta su uso como medio de pago, que es una de las funciones básicas del dinero. Además, no están sujetas a ningún tipo de regulación ni supervisión. Por ello, es necesario promover la difusión de las advertencias acerca de los riesgos que entraña su emisión y utilización.

2. Estudiar los aspectos relacionados con la prevención del blanqueo de capitales. Entre otros, considerar a los proveedores de servicios de cambio de moneda virtuales por monedas fiduciarias y a los prestadores de servicios de custodia de claves (monederos virtuales) como entidades sujetas a la regulación de blanqueo de dinero quedando obligadas a la identificación de sus clientes.

---

[430] Como se señaló anteriormente, el uso de las criptomonedas se ha difundido mucho en los últimos diez años, siendo *Bitcoin* la más conocida y *Blockchain* (o cadena de bloques) la tecnología que se utilizó para desarrollarla. *Bitcoin* fue la primer criptomoneda, se creó en el año 2008 por Satoshi Nakamoto quien explica en detalle el funcionamiento en el "*Bitcoin Paper*"**,** donde define –entre otras cosas– a la moneda electrónica como una cadena de firmas electrónicas, que no depende de la confianza de una entidad central, que crea una red de usuario a usuario, que registra una historia pública de transacciones, distribuida, encriptada, irresoluble y que no puede ser modificada. Actualmente hay más de 2000 criptomonedas diferentes.

[431] ING. Nota de prensa, URL: https://www.ing.es/sobre-ing/prensa/pdf/260518.pdf consultado el 20 de julio de 2019.

3. Estudiar los aspectos fiscales del uso de las criptomonedas para evitar cualquier tipo de evasión.

4. Seguir apoyando y participando en los grupos de trabajo creados en el seno de la Comisión Nacional del Mercado de Valores (CNMV) y del Banco de España o los que se puedan crear en las instituciones europeas, para el estudio de las implicaciones del uso de las criptomonedas.

5. Hasta que exista una regulación global, advertir a los usuarios del componente especulativo, de los fraudes y del riesgo de burbujas de las criptomonedas, así como la necesidad de ser prudente en su utilización.[432]*"*

Por otra parte, cabe hacer mención a un comunicado conjunto que hicieron en febrero de 2018 el Banco de España y la Comisión Nacional del Mercado de Valores (CNMV) sobre la temática, donde destacan, entre otras cosas, que[433]: "*Las "criptomonedas" así como los distintos actores implicados en su comercialización directa, no están regulados en la Unión Europea. Esto implica que si una persona compra o mantiene "criptomonedas" no se beneficia de las garantías y salvaguardias asociadas a los productos financieros regulados.*

Asimismo, ya sea por cómo están estructurados o por dónde se encuentre la residencia de sus emisores, los "tokens" emitidos en una ICO o los productos financieros referenciados a "criptomonedas" podrían no estar sujetos a regulación." (...)

"En muchas ocasiones los distintos actores implicados en la emisión, custodia y comercialización de "criptomonedas" (plataformas de intercambio, emisores de ICOs, proveedores de carteras digitales, etc.) no se encuentran localizados en España, de modo que la resolución de cualquier conflicto podría quedar fuera del ámbito competencial de las autoridades españolas y estaría sujeto al marco normativo del país en cuestión."

---

[432] Boletín Oficial de las Cortes Generales, Senado, 12 de febrero de 2018. URL: http://www.senado.es/legis12/publicaciones/pdf/senado/bocg/BOCG_D_12_201_1588.PDF Consultado el 20 de julio de 2019.

[433] Comunicado conjunto del Banco de España y la CNMV del 8 de febrero de 2018. URL: https://www.cnmv.es/loultimo/NOTACONJUNTAriptoES%20final.pdf Consultado el 20 de julio de 2019.

Asimismo, destacan el elevado riesgo de perder el capital invertido, que hay problemas de iliquidez y volatilidad extrema, así como de información inadecuada. Indican que: *"Las "criptomonedas" carecen de valor intrínseco, convirtiéndose en inversiones altamente especulativas. Asimismo, su fuerte dependencia de tecnologías poco consolidadas no excluye la posibilidad de fallos operativos y amenazas cibernéticas que podrían suponer indisponibilidad temporal o, en casos extremos, pérdida total de las cantidades invertidas.*

En su mayoría, las ICOs están asociadas a proyectos empresariales en etapas muy tempranas de desarrollo, sin que exista un modelo de negocio consolidado o con flujos de caja inciertos. Estas iniciativas pueden tener una alta probabilidad de fracaso.

Las inversiones en "criptomonedas" o en ICOs al margen de la regulación no están protegidas por ningún mecanismo similar al que protege el efectivo o los valores depositados en entidades de crédito y empresas de servicios de inversión (en el caso de efectivo o valores depositados en entidades de crédito o empresas de servicios de inversión, con arreglo a ciertas condiciones, los correspondientes fondos de garantía aseguran importes de hasta 100.000 euros)." (...)

"La ausencia de mercados equiparables a los mercados organizados de valores sujetos a regulación puede dificultar la venta de "criptomonedas" o de "tokens" emitidos en ICOs para obtener efectivo convencional. Sus propietarios pueden no disponer de opciones en el momento deseado para convertir en moneda convencional sus criptomonedas o recuperar su inversión. Y cuando existe la posibilidad de vender estos activos, puede haber falta de transparencia en relación con las comisiones aplicables y además su precio suele sufrir fuertes oscilaciones sin causa objetiva aparente." (...)

"En el caso de las ICOs, la información que se pone a disposición de los inversores no suele estar auditada y, con frecuencia, resulta incompleta. Generalmente, enfatiza los beneficios potenciales, minimizando las referencias a los riesgos. Además, el lenguaje utilizado suele tener un carácter muy técnico y, en ocasiones, poco claro, por lo que no es fácil conocer la entidad y naturaleza de los riesgos que se asumirían con la inversión y ésta puede resultar inapropiada para las necesidades y perfiles de riesgo de los clientes."

Por otra parte, en línea con la ICOs y diversas formas de financiar emprendimientos, en los últimos años se desarrolló el "crowdfunding" como una forma alternativa para conseguir financiación.

(II.3.D.) Modalidades de financiación colectiva.

En el 2015 se dictó la Ley Nº 5/2015, de 27 de febrero, de Fomento de la Financiación Empresarial.

Como surge del preámbulo: *"La función última del sistema financiero y su aportación más definitiva a la actividad económica consiste en la canalización eficiente de recursos desde los agentes con capacidad de ahorro hacia aquellos que necesitan financiación. Esta transmisión del ahorro hacia la inversión se puede producir de manera intermediada a través de entidades bancarias, o bien a través del acceso directo a los mercados de capitales, que relacionan inversores y demandantes de financiación. El correcto funcionamiento y la adecuada regulación de ambos canales son dos de los parámetros determinantes del crecimiento económico y la creación de empleo."*

Partiendo de dicha base, se destaca que las empresas españolas han dependido mucho de la financiación bancaria, que en los últimos años el volumen de crédito ha bajado y ha aumentado el costo, lo cual afecta a las PYME. En este sentido, se pretende: (1) hacer más accesible y flexible la financiación bancaria a las PYME, y (2) desarrollar medios alternativos de financiación, para lo cual se deben fortalecer las fuentes de financiación no bancaria.

Se considera que para que el sistema económico se desarrolle y avance, se requiere de mercados de capitales con bases sólidas y estables, q ofrezcan fondos para la producción y para la economía real. Además fomentan la diversificación de las fuentes de financiación, reduciendo la vulnerabilidad de la economía ante las crisis crediticias. En este contexto, entre las diversas medidas que se adoptan, se establece el régimen jurídico para las plataformas de financiación colectiva o *crowdfunding*. Se ven a estas plataformas como un mecanismo de desintermediación financiera, desarrollado sobre la base de las nuevas tecnologías, que tiene diversas figuras. Se regula específicamente aquella en la que el inversor espera recibir una remuneración dineraria por su participación, no alcanzando a las otras modalidades, como puede ser el de compraventa o donación.

"Las plataformas de financiación participativa ponen en contacto a promotores de proyectos que demandan fondos mediante la emisión de valores y participaciones sociales o mediante la solicitud de préstamos, con inversores u ofertantes de fondos que buscan en la inversión un rendimiento. En dicha actividad sobresalen dos características, como son la participación masiva de inversores que financian con cantidades reducidas pequeños proyectos de alto potencial y el carácter arriesgado de dicha inversión. Si bien podría pensarse que son pequeños inversores los que financian por acumulación proyectos en estas plataformas, las experiencias internacionales apuntan a que los inversores profesionales, aquí denominados inversores acreditados, apuestan también por los proyectos de financiación participativa, prestando las plataformas que los publican un útil servicio de filtrado de proyectos potencialmente viables.[434]"

Se regula desde tres ángulos:

(1) Régimen jurídico de las plataformas de financiación participativa: tienen requisitos de autorización y de registro ante la CNMV.

(2) Actividad de las entidades autorizadas, concurriendo los principios de necesidad y proporcionalidad, buscando asegurar la neutralidad de las plataformas en su relación entre inversores y promotores.

(3) Clarifican las normas que aplican para quienes utilicen este canal de financiación, se busca potenciar la actividad y proteger al inversor. Entre las medidas, se prohíbe el asesoramiento financiero y tomar fondos destinados a realizar pagos en nombre propio por cuenta de clientes, sin contar con la autorización preceptiva de la entidad de pago. Por otra parte, a fin de reducir el riesgo, se establecen límites al volumen que cada proyecto puede captar a través de una plataforma de financiación participativa, los límites a la inversión máxima que un inversor no acreditado puede realizar y las obligaciones de información para que toda decisión de inversión haya podido ser debidamente razonada. Adicionalmente, se exige una expresión del inversor por la que manifieste que ha sido debidamente advertido de los riesgos, para asegurar una voluntad consciente y bien informada.

[434] Preámbulo de la Ley 5/2015, URL: https://www.boe.es/buscar/act.php?id=BOE-A-2015-4607 Consultado el 20 de julio de 2019.

Considerando lo expuesto, el artículo 46 de la Ley 5/2015 define a las plataformas de financiación participativa señalando que son *"empresas autorizadas cuya actividad consiste en poner en contacto, de manera profesional y a través de páginas web u otros medios electrónicos, a una pluralidad de personas físicas o jurídicas que ofrecen financiación a cambio de un rendimiento dinerario, denominados inversores, con personas físicas o jurídicas que solicitan financiación en nombre propio para destinarlo a un proyecto de financiación participativa, denominados promotores."*

No comprenden los casos en que la financiación captada sea a través de donaciones, ventas de bienes y servicios, y préstamos sin interés.

La regulación alcanza a aquellas plataformas que realicen su actividad en territorio español. No se considerará que el servicio ha sido en territorio español cuando un residente en España participa por iniciativa propia como inversor o promotor, si la plataforma tiene domicilio social en el extranjero. Además, no se entiende que la actividad se pone en marcha a iniciativa propia cuando la empresa anuncie, promocione o capte clientes o posibles clientes en España, y cuando la empresa dirija sus servicios especialmente a inversores y promotores que residan en España[435].

Solo podrán realizar la actividad aquellas plataformas que hayan sido autorizadas y estén inscritas en el registro de la CNMV. Asimismo, deben: (i) tener por objeto social exclusivo la realización de las actividades que sean propias a las plataformas de financiación participativa; (ii) tener su domicilio social, su administración y dirección en España o en otro Estado miembro; (iii) revestir la forma de sociedad de capital, por tiempo indefinido; (iv) disponer de un capital social en efectivo de al menos 60.000 euros, o un seguro de responsabilidad profesional, un aval u otra garantía equivalente con una cobertura mínima de 300.000 euros por reclamación de daños y un total de 400.000 euros anuales para todas las reclamaciones, o una combinación de capital inicial y de seguro de responsabilidad civil profesional aval u otra garantía equivalente; (v) los administradores deben ser personas reconocidas por su honorabilidad empresarial o profesional, con conocimiento y experiencia adecuada en la materia; (vi) disponer de buena organización administrativa y contable o de procedimientos de

[435] Artículo 47 de la Ley Nº 5/2015.

control interno adecuados; (vii) disponer de un reglamento interno de conducta[436]; (viii) prever mecanismos para que, ante el cese de la actividad, sigan prestando los servicios ya comprometidos. [437]

Los proyectos de financiación participativa deben: "*(a) estar dirigidos a una pluralidad de personas físicas o jurídicas que, invirtiendo de forma profesional o no, esperan obtener un rendimiento dinerario. (b) Realizarse por promotores, personas físicas o jurídicas, que solicitan la financiación en nombre propio. (c) Destinar la financiación que se pretende captar exclusivamente a un proyecto concreto del promotor, que solo podrá ser de tipo empresarial, formativo o de consumo sin que en ningún caso pueda consistir en: 1.º La financiación profesional de terceros y en particular la concesión de créditos o préstamos. 2.º La suscripción o adquisición de acciones, obligaciones y otros instrumentos financieros admitidos a negociación en un mercado regulado, en un sistema multilateral de negociación o en mercados equivalentes de un tercer país. 3.º La suscripción o adquisición de acciones y participaciones de instituciones de inversión colectiva o de sus sociedades gestoras, de las entidades de capital riesgo, otras entidades de inversión colectiva de tipo cerrado y las sociedades gestoras de entidades de inversión colectiva de tipo cerrado. (d) Financiarse a través de algunas de las formas previstas en el artículo 50 de esta Ley*[438]*.*[439]*"*

[436] "que contemple, en particular, los posibles conflictos de interés y los términos de la participación de los administradores, directivos, empleados y apoderados en las solicitudes de financiación que se instrumenten a través de la plataforma" (Artículo 55.h de la Ley 5/2015).
[437] Artículo 55 de la Ley 5/2015.
[438] El artículo 50 dispone las formas de financiación participativa. Prevé que*:*
"1. Los proyectos de financiación participativa podrán instrumentarse a través de:

a) La emisión o suscripción de obligaciones, acciones ordinarias y privilegiadas u otros valores representativos de capital, cuando la misma no precise y carezca de folleto de emisión informativo al que se refieren los artículos 25 y siguientes de la Ley 24/1988, de 28 de julio, del Mercado de Valores. En este caso, se entenderá por promotor a la sociedad que vaya a emitir los valores.
Cuando en la financiación participen inversores no acreditados tal y como se definen en este título, los valores a los que se refiere este apartado no podrán incorporar un derivado implícito.
b) La emisión o suscripción de participaciones de sociedades de responsabilidad limitada, en cuyo caso se entenderá por promotor a la sociedad de responsabilidad limitada que vaya a emitir las participaciones.
c) La solicitud de préstamos, incluidos los préstamos participativos, en cuyo caso se entenderá por promotor a las personas físicas o personas jurídicas prestatarias.

En definitiva, actualmente se entiende que hay dos tipos: (1) crowdfunding en el que el inversor a cambio de su inversión recibe valores emitidos por el promotor, y (2) crowdlending en el que se recibe un rendimiento a cambio del dinero prestado.

Además se establecen diversos tipos de inversores: los profesionales y los no profesionales. *"En teoría, la plataforma que publica el proyecto no puede tener a un inversor no profesional invirtiendo más de 3.000€ por proyecto y un máximo de 10.000€ al año. Los inversores profesionales sí pueden invertir más, pero han de acreditar ser profesionales.*[440] *"*

La norma regula múltiples aspectos de la actividad. Entre las diversas críticas que tuvo la norma, se destacó que se reguló la modalidad sin entenderlo[441], que dejó afuera de la regulación las modalidades más usadas como es la participación por recompensa, y se compara con la regulación de Inglaterra que se realizó en diálogo constante con la industria, generando mayores beneficios.

(III) Regulación en Uruguay

Uruguay no dispone de una normativa única que trate sobre la temática, cuenta con diversos instrumentos legales y normativos que pretenden atender aspectos puntuales de los diversos desafíos que conlleva la sociedad de la información. Como se verá la normativa y las soluciones propuestas en el ordenamiento jurídico español se encuentran bastante más desarrolladas que las de Uruguay.

---

2. La solicitud de préstamos a través de la publicación de proyectos en las plataformas de financiación participativa, en los términos previstos en esta Ley, no tendrá la consideración de captación de fondos reembolsables del público."

[439] Artículo 49 de la Ley

[440] MORENO, DANIEL, "¿Qué es el crowdfunding y cómo se regula?", URL: https://www.lacentraldelnegocio.com/que-es-crowdfunfing-como-se-regula/ Consultado el 20 de julio de 2019.

[441] *"Cuando en España se reguló el crowdfunding [mecanismo colectivo de financiación de proyectos] en 2015, el regulador lo hizo sin entender", introduce el responsable en España y en el sur de Europa de Crowdcube, Pepe Borrell. "En Reino Unido, cuando se aprobó el eqUITy crowdfunding [mecanismo de inversión en empresas privadas] y el crowdlending [mecanismo para poner en contacto a prestamistas con prestatarios], en 2012,* ***lo primero que hubo fue un periodo de prospección: reuniones con todas las plataformas, periodo de entender, de percibir el feeling****... y el equipo que se reunía con ellas estaba formado por analistas y por gente muy competente que entendió cómo trabajábamos y decidió crear una regulación para asegurar que las cosas se hicieran bien, sin hundir a los agentes que operaban en el sector". EL MUNDO: "En España se reguló el "crowdfunding" sin entenderlo". URL:* https://www.elmundo.es/economia/innovadores/2019/01/30/5c4f3283fdddff068c8b45e9.html Consultado el 20 de julio de 2019.

(III.1.) Servicios prestado mediante el uso de medios informáticos y aplicaciones tecnológicas

En marzo de 2016 el Poder Ejecutivo presentó al Parlamento un proyecto de ley denominado "*Servicios prestados mediante el uso de medios informáticos y aplicaciones tecnológicas*", por el cual se busca regular las actividades de los prestadores que emplean medios informáticos y aplicaciones tecnológicas para conectar diversos servicios.

Conforme surge del mensaje que acompañó al proyecto de ley: "La aparición en nuestro país de ciertas modalidades de contratación de servicios a través de plataformas informáticas, obliga a efectuar ajustes al ordenamiento jurídico que permitan acompasar esos cambios, evitando de este modo, una desregulación no querida, que distorsione el mercado, y vaya en detrimento de los consumidores y de la competencia de otros sujetos *que prestan servicios similares de forma "tradicional", encontrándose sometidos a diversas formas de contralor".*[442]

Tras un amplio debate que reconoció la necesidad del país de trabajar sobre la "*era de la economía digital*", la Comisión de Innovación, Ciencia y Tecnología de la Cámara de Representantes aprobó, a fines del 2016, un proyecto de ley, que le hace ajustes al proyecto original remitido por el Poder Ejecutivo.

El proyecto aprobado busca que sea una norma minimalista, que regule con generalidad, atendiendo la cuestión como una actividad a alentar y de interés general. Entienden que no se debe distinguir el medio de prestación del servicio, brindando certezas a partir de la fijación de reglas de juego claras, en aplicación del principio de igualdad ante la ley y de defensa de la competencia.

El ámbito subjetivo del proyecto aprobado es: *"todos los servicios prestados en el territorio nacional, a título oneroso, que utilizan para su contratación una plataforma informática de intermediación",* disponiendo que *"Dichos servicios estarán sujetos a las disposiciones del ordenamiento jurídico que les sean de aplicación, en función de la*

442 Proyecto de Ley remitido por el Poder Ejecutivo en marzo de 2016. URL: https://parlamento.gub.uy/documentosyleyes/ficha-asunto/128667/tramite

actividad que desarrollen, con independencia de la utilización de medios electrónicos de contratación".[443]

El proyecto establece principios generales que, junto con el Título Preliminar del Código Civil, servirán como criterio interpretativo en la aplicación de la ley. Los principios generales establecidos son los siguientes:[444]

a. Equivalencia funcional: *"los servicios contratados por medios electrónicos no estarán sujetos a regulación jurídica diferencial como consecuencia del medio de contratación utilizado".*

b. lnalteración del Derecho preexistente: *"considerándose los servicios como equivalentes, se aplicará a los servicios contratados por medios electrónicos la misma regulación jurídica que a los contratados por cualquier otro medio".*

c. Libre competencia: "*Aplicarán los principios de eficiencia, no discriminación regulatoria, ausencia de requisitos injustificados o barreras a la entrada que impidan el ingreso de nuevos agentes al mercado o que establezcan obstáculos para el desarrollo de nuevos modelos de negocios".*

Asimismo, el proyecto aclara que, en lo que respecta a las relaciones de trabajo o a cualquier otro vínculo que se realice para la prestación de los servicios, así como lo vinculado al contralor, se regirán por todas las normas vigentes que les sean de aplicación, como ser las laborales, administrativas, previsionales, tributarias y cualquier otra a la que se encuentren sujetos los servicios o las actividades a desarrollar.

Por otra parte, entre otras disposiciones, el proyecto establece la obligación de los titulares de las plataformas de disponer de forma permanente, fácil, directa y gratuita, tanto para los destinatarios de los servicios, como para los órganos competentes, del adecuado acceso a la información que establezca la reglamentación.

Entre lo más criticado del proyecto, se destaca lo vinculado al contralor. El proyecto señala que los organismos de contralor del Estado deben comunicar a la Justicia cualquier incumplimiento en el que incurran los sujetos pasivos en un plazo de tres días, desde que haya quedado ejecutoriada la resolución del procedimiento

443 Artículo 2° del Proyecto de Ley aprobado por la Cámara de Representantes el 13 de diciembre de 2016, carpeta 731/2016.

444 Artículo 3° del Proyecto de Ley aprobado por la Cámara de Representantes el 13 de diciembre de 2016, carpeta 731/2016.

administrativo que haya entendido configurado el incumplimiento. Una vez comunicado, se prevé que el Magistrado puede adoptar las medidas cautelares que entienda pertinentes, tales como el bloqueo de las transferencias de fondos o la imposibilidad de concretar cualquier otra operación, desde y hacia las cuentas bancarias de los incumplidores. Finalmente, señala que los sujetos pasivos afectados por la decisión judicial mencionada precedentemente, podrán recurrirla, con los medios impugnativos que al efecto establecen las normas procesales.

Resulta evidente que, el hecho de que ante "cualquier incumplimiento" se puedan tomar medidas tan gravosas, tales como el bloqueo de las transferencias de fondos o la imposibilidad de concretar cualquier otra operación desde y hacia las cuentas bancarias, no parecería estar acorde con los principios de proporcionalidad, de razonabilidad, ni con el supuesto fin de alentar la actividad.

En este sentido, se presentaron muchas críticas al proyecto, sobre todo por el riesgo de que pueda frenar el desarrollo de la economía digital, haciendo énfasis en la importancia de promoverla.

Entre las diversas reacciones, vale destacar que la Cámara Uruguaya de Tecnologías de la Información (CUTI) y la Cámara de Economía Digital de Uruguay (CEDU) presentaron un proyecto de ley que, entre otras cosas: (i) declara de interés nacional las actividades vinculadas a la economía colaborativa, (ii) dispone como objeto de la norma impulsar el desarrollo económico y sustentable del país, promoviendo la creación de emprendimientos con base en plataformas colaborativas, (iii) establece que "*el desarrollo de plataformas colaborativas*" debe ser considerado a todos los efectos como "*producción de soporte lógico y servicios vinculados*", que se entiende como "*una plataforma en línea que conecta a los prestadores (que ofrecen bienes y servicios de manera ocasional o que actúan a título profesional) con los usuarios y facilitan las transacciones entre ellos*", y que cuando brinden otro tipo de servicios, estarán sujetas a la normativa específica del sector de actividad en que se desempeñen[445].

445 Proyecto de Ley presentado por CEDU y CUTI: https://www.cedu.org.uy/pub/cedu-y-cuti-presentaron-proyecto-de-ley-para-promover-la-econom %C3 %ADa-colaborativa

Al momento no se aprobó la normativa específica, mas como veremos a continuación, si se adoptaron diversas normativas vinculadas a aspectos tributarios y a otros temas relacionados con medios de pagos electrónicos.

(III.2.) Aspectos tributarios

Uruguay fue uno de los primeros países en regular lo referente a los aspectos tributarios de las plataformas digitales.

En primer lugar a través del artículo 731 de la Ley Nº 19.355, se dispuso que aquellas entidades, residentes o no, que intervengan, directa o indirectamente, en la oferta o en la demanda de la prestación de servicios de transporte terrestre de pasajeros o de alojamiento turísticos, así como en los servicios de arrendamiento de inmueble, por personas que no estén debidamente habilitadas para el desarrollo de tales actividades; serían solidariamente responsables por los tributos y sanciones pecuniarias aplicables.

A los efectos de dicho artículo, se señaló que se entendería por intervención en la oferta o en la demanda de la prestación de servicios, a todas aquellas actividades, realizadas a título gratuito u oneroso, a través de cualquier medio, incluida la utilización de aplicación informáticas, que cumplan con alguna de las siguientes condiciones:

a tengan por objeto la medicación o intermediación en la prestación de los servicios mencionados;

b suministren a los prestadores o a los usuarios datos de los servicios aludidos, a efectos de que una o ambas partes dispongan de información necesaria para acordar la prestación.

Posteriormente, se aprobó la Ley Nº 19.535 por medio de la cual se introdujeron cambios a los Títulos 4 (Impuesto a las Rentas de las Actividades Económicas: IRAE), 8 (Impuesto a las Rentas de los No Residentes: IRNR) y 10 (Impuesto al Valor Agregado: IVA) del Texto Ordenado de 1996; siendo reglamentada por el Ministerio de Economía y Finanzas en Decreto Nº 144/2018[446] y complementada por la Resolución de la Dirección General de Impositiva Nº 9270/2018.

446 https://medios.presidencia.gub.uy/legal/2018/decretos/05/mef_1835.pdf

Como explican Nicolás Juan y Cecilia Arias[447], la dificultad principal que se plantea en este tipo de actividades, *"es que las mismas son generalmente desarrolladas por entidades no residentes con un componente tecnológico elevado, por lo que hace posible que se realicen un número importante de operaciones en un determinado territorio aún sin manifestar presencia física en el mismo".*

En este sentido, se agregaron disposiciones relacionadas con las rentas de: i. actividades internacionales de producción, distribución e intermediación de películas cinematográficas y otras transmisiones audiovisuales, y ii. las actividades de mediación e intermediación realizadas a través de medios informáticos.

Respecto a las rentas derivadas de:

i. *la producción, distribución o intermediación de películas cinematográficas y de tapes, así como las derivadas de la realización de transmisiones directas de televisión y de transmisión de cualquier contenido audiovisual, incluidas las realizadas a través de Internet, plataformas tecnológicas, aplicaciones informáticas, u otros medios similares, tales como acceso y descarga de películas*: serán consideradas íntegramente de fuente uruguaya siempre que el demandante se encuentre en territorio nacional.

Se entenderá que el demandante se encuentra en territorio nacional cuando se localice en el mismo: (a) la dirección de IP (Protocolo de Internet) del dispositivo utilizado para la contratación del servicio o (b) su dirección de facturación. En caso de prestaciones de servicios de tracto sucesivo, la determinación de la localización del demandante, deberá realizarse al momento de la contratación del referido servicio.

Si no se verifica al menos una de las circunstancias de localización, se presumirá –salvo prueba en contrario– cuando la contraprestación del servicio se efectúe a través de medios de pago electrónico administrados desde nuestro país, tales como instrumentos de dinero electrónico, tarjetas de crédito o débito, cuentas bancarias, o los instrumentos análogos a que refiere el artículo 4º del Decreto Nº 203/014 de 22 de julio de 2014[448].

---

447 JUAN, NICOLÁS Y ARIAS, CECILIA: "Uruguay lidera tributación para plataformas digitales". URL: https://www.uruguayxxi.gub.uy/es/noticias/articulo/uruguay-lidera-tributacion-para-plataformas-digitales/ Consultado el 15 de enero de 2019.

448 Artículo 4º del Decreto Nº 203/2014: *"Instrumentos análogos. Se considerarán instrumentos análogos a las tarjetas de débito y a los instrumentos de dinero electrónico los siguientes: a) los débitos automáticos en cuentas en instituciones de intermediación financiera,*

Se considerará que existen actividades ejercidas parcialmente dentro del territorio nacional, aun cuando sean realizadas sin presencia física en el mismo.

Por otra parte, en relación al IVA, se considerarán gravadas cuando los servicios sean consumidos o utilizados en el país.

ii. las "*actividades de mediación e intermediación realizadas a través de medios informáticos"*, se entiende que son aquellas que: (a) por su naturaleza, estén básicamente automatizadas, requieran una intervención humana mínima, y que no tengan viabilidad al margen de la tecnología de la información, y (b) aquellas que impliquen la intervención, directa o indirecta, en la oferta o en la demanda de la prestación de servicios.

Asimismo, se entiende por "*tecnología de la información*" al uso de equipos de telecomunicaciones o dispositivos electrónicos para la transmisión, el procesamiento o almacenamiento de datos.

A efectos de definir el lugar donde se encuentra el demandante y el oferente de los servicios, se considerará su ubicación al momento de contratar la mediación o la intermediación, según corresponda. Se entiende que se encuentran en territorio nacional:

i. El oferente, cuando el servicio se presta en dicho territorio.

ii. El demandante, cuando se localice en dicho territorio la dirección de IP del dispositivo utilizado para la contratación del servicio de mediación o intermediación o su dirección de facturación.

Si no se configura alguno de esos dos supuestos, se presumirá –salvo prueba en contrario– que el demandante se encuentra en territorio nacional cuando la contraprestación del servicio se efectúe a través de medios de pago electrónico administrados desde nuestro país, tales como instrumentos de dinero electrónico,

---

incluyendo los que se realicen en las tarjetas de débito; b) los débitos automáticos en instrumentos de dinero electrónico; c) las tarjetas prepagas que no constituyan instrumentos de dinero electrónico, siempre que sean emitidas por entidades reguladas y supervisadas por el Banco Central del Uruguay que cuenten con autorización del mismo para emitir dichos instrumentos; d) los pagos electrónicos efectuados a través de cajeros automáticos, teléfonos celulares o por Internet, con fondos almacenados en cuentas en instituciones de intermediación financiera, en instrumentos de dinero electrónico o en tarjetas prepagas que cumplan con lo previsto en el literal anterior."

tarjetas de crédito o debido, cuentas bancarias, o los instrumentos a que se refiere el artículo 4º del Decreto Nº 203/014 de 22 de julio de 2014.

Se considera que existen actividades desarrolladas parcialmente dentro del territorio nacional, aun cuando las mismas sean realizadas sin presencia física en el mismo.

"En este caso la ley determinó dos porcentajes de gravamen para el IRNR, dependiendo del lugar donde se encuentren el oferente y el demandare del servicio. De esta manera, si ambos se encuentran en territorio nacional la renta se considera 100 % de fuente uruguaya, mientras que si solo uno de ellos se encuentra en territorio nacional, se considerará sólo el 50 % de fuente uruguaya. (…) Con respecto al IVA, los criterios de determinación del gravamen dependerán también de la ubicación del oferente y el *demandante, pudiendo estar alcanzada la contraprestación entonces por el impuesto al 50 % o al 100 %".*[449]

(III.3.) Pagos y dinero electrónicos, monedas digitales y modalidades de financiación colectiva.

(III.3.A) Pagos electrónicos

En lo que respecta a la prestación de los servicios financieros en Uruguay, hay múltiples normas que conforman el marco jurídico y que deben considerarse dependiendo el tipo de servicio que se vaya a prestar. Entre las diversas normas, se destacan principalmente la Ley de Intermediación Financiera, Nº 15.322, la Carta orgánica del BCU, la Ley de Mercado de Valores (Ley Nº 18627) y la Ley de Inclusión Financiera, Nº 19.210.

Como surge de la Exposición de Motivos remitida por el Poder Ejecutivo, que acompañó al proyecto de ley de la actual Ley Nº 19.210, conocida como "Ley de Inclusión Financiera": *"Las políticas de inclusión financiera contribuyen al desarrollo económico y social y, en particular, constituyen un importante aporte para mejorar las condiciones de vida de las población y potenciar las actividades de las micro, pequeñas y medianas empresas (...).*

...El sistema financiero constituye uno de los pilares fundamentales por donde se canaliza los recursos financieros generados por la sociedad. Por ese motivo, uno de los

449 JUAN, NICOLÁS Y ARIAS, CECILIA, obra citada.

objetivos centrales de las políticas públicas es contribuir a lograr un sistema financiero más desarrollado, más profundo, más transparente, más competitivo y más inclusivo, para de esta manera potenciar su contribución al logro de un mayor desarrollo económico y social, sobre bases de equidad e inclusión (…).

La inclusión financiera plena implica que todas las personas y empresas puedan tener acceso a una amplia gama de servicios financieros de calidad, proporcionados a precios accesibles y de manera conveniente para los clientes, adecuados a sus necesidades."

De lo anterior se desprende el rol clave que tiene para la inclusión el desarrollo del sistema financiero, destacando a continuación la Exposición de Motivos, que para su adecuado desarrollo necesita, entre otras cosas, de: (i) una adecuada regulación y supervisión financiera, (ii) una amplia oferta de productos y servicios financieros de calidad, a precios razonables, que se adapten a las necesidades de las personas y de las empresas, (iii) una amplia red física y tecnológica, con acceso a canales de transacciones tradicionales y no tradicionales, que permitan realizar transacciones de forma segura y eficiente, (iv) la promoción y el desarrollo de políticas de educación financiera, y (v) la protección al usuario de los servicios financieros y la transparencia de la información.

Entre los objetivos de la norma se señalan: (1) Universalizar derechos y avanzar en la democratización del sistema financiero. (2) Promover la competencia en el sector, permitiendo la incorporación de nuevos actores que ofrezcan servicios de pago. (3) Fomentar el uso de los medios de pago electrónicos en sustitución del efectivo. (4) Estimular la conducta de ahorro de la población.

En este sentido, en relación a los medios de pagos electrónicos, el artículo 1 de la Ley Nº 19.210 dispone: "*Se entenderá por medio de pago electrónico las tarjetas de débito, las tarjetas de crédito, los instrumentos de dinero electrónico y las transferencias electrónicas de fondos, así como todo otro instrumento análogo que permita efectuar pagos electrónicos a través de cajeros automáticos, por Internet o por otras vías, de acuerdo a lo que establezca la reglamentación.*

Los pagos efectuados a través de medios de pago electrónicos tienen pleno efecto cancelatorio sobre las obligaciones en cumplimiento de las cuales se efectúan".

Como surge de la definición de "medio de pago electrónico", el concepto es amplio, pudiendo considerarse como medio de pago todo instrumento que permita efectuar pagos electrónicos a través de cajeros automáticos, por Internet o por otras vías.

El 28 de diciembre de 2018 el Paramento aprobó la Ley Nº 19.731, por medio de la cual regula el funcionamiento de los medios de pago electrónico, que hayan sido emitidos por instituciones locales.

A estos efectos, entiende por medio de pago electrónicos a los siguientes: (i) tarjeta de débito: permite a su titular realizar compras de bienes, pagos de servicios y extracción de efectivo a ser debitada directamente de los fondos que mantiene en una cuenta en una institución de intermediación financiera; (ii) instrumentos de dinero electrónico: se remite al artículo 2 de la Ley Nº 19.210, se comentará a continuación, señalando que tendrá el mismo funcionamiento que las tarjetas de crédito; y (iii) tarjeta de crédito: habilita a su titular a hacer uso de una línea de crédito otorgada, que le permite realizar compras de bienes, pagos de servicios y extracción de efectivo hasta un límite previamente acordado[450].

Entre los sujetos intervinientes en el sistema de medios de pago electrónico, la Ley señala a los siguientes: (i) Emisor: institución regulada por el Banco Central del Uruguay que emite tarjetas de crédito, de débito o instrumentos de dinero electrónico; (ii) Adquirente: entidad que celebra contratos de afiliación con los comercios adheridos al sistema; (iii) Comercio: sujeto de derecho que se haya adherido al sistema a través de la firma de un contrato con el adquirente; y (iv) Usuario: sujeto de derecho que, de acuerdo a lo previsto en el contrato con el emisor, se encuentra habilitado para el uso de los medios de pago electrónico[451].

Se regulan diversos aspectos relacionados con transacciones que se realizan de forma presencial, considerando los diversos vínculos que se generan entre: (i) adquirente y comercio, (ii) comercio y usuario, (iii) emisor y comercio, (iv) usuario y emisor.

En relación a los contratos a celebrar entre:

450 Artículo 1 de la Ley Nº 19.731.
451 Artículo 2 de la Ley Nº 19.731.

i. Adquirente y comercios: se tendrá en cuenta especialmente aspectos vinculados con: defensa de la competencia, no discriminación, plazos de pago, la comisión, arancel o tasa de descuento, plazos para presentar información sobre las operaciones a efectos de su liquidación y libertad de elegir la opción de único pago. Por su parte, el comercio debe aceptar los medios de pago incluidos en el contrato celebrado, debe verificar si corresponde la identidad del usuario, e informar de la comisión de cualquier ilícito o hecho irregular que pueda poner en riesgo el funcionamiento del sistema en que opera el medio de pago electrónico.

ii. Comercio y usuario: cuando corresponda el comercio controlará la identidad del usuario, con la diligencia de un buen hombre de negocios, no pudiendo almacenar ningún dato personal o hábito de consumo del usuario sin su consentimiento.

iii. Emisor y comercio: autorizada una operación de pago, el emisor será responsable de cualquier incumplimiento por parte del usuario, lo mismo en caso de clonación. En caso de que el emisor celebre acuerdo comerciales promocionales, que excluya a determinados comercios de un mismo sector de actividad, la Comisión de Promoción y Defensa de la Competencia actuará de oficio o a denuncia de parte.

iv. Usuario y emisor: el usuario puede resolver las compras realizadas conforme al artículo 16 de la Ley Nº 17.250 (compra de productos y servicios fuera del local comercial), comunicando la situación al emisor. Los contratos deben estar redactados en español, salvo excepciones, utilizando caracteres fácilmente legibles, lenguaje claro y toda otra característica que facilite su comprensión. Se perfeccionará con el consentimiento del usuario y el envío de medios de pago electrónico no solicitados se regirá por lo establecido en el literal D del artículo 22 de la Ley Nº 17.250 (prácticas abusivas). La ley prevé ciertas cláusulas y prácticas que se consideran como abusivas, así como aspectos mínimos que se deben incluir en los contratos. Asimismo, prevé obligaciones y responsabilidades del emisor; y responsabilidades de los usuarios.

(III.3.B.) Dinero electrónico

Se considera un medio de pago electrónico.

El artículo 2 de la Ley Nº 19.210 lo define como aquellos instrumentos representativos de un valor monetario exigible a su emisor, tales como tarjetas prepagas, billeteras electrónicas u otros instrumentos análogos, de acuerdo a lo que establezca la reglamentación, con las siguientes características:

a. El valor monetario es almacenado en medios electrónicos, tales como un chip en una tarjeta, un teléfono móvil, un disco duro de una computadora o un servidor.

b. Es aceptado como medio de pago por entidades o personas distintas del emisor y tiene efecto cancelatorio.

c. Es emitido por un valor igual a los fondos recibidos por el emisor contra su entrega.

d. Es convertible a efectivo a solicitud del titular, según el importe monetario del instrumento de dinero electrónico emitido no utilizado.

e. No genera intereses.

Se exceptúa de lo dispuesto en el literal D señalado las prestaciones de alimentación previstas en el artículo 167 de la Ley Nº 16.713.

La norma dispone que podrán emitir dinero electrónico las instituciones de intermediación financiera y las instituciones emisoras de dinero electrónico, habilitadas a tales efectos por el Banco Central del Uruguay.

Además el artículo 4 de la Ley Nº 19.210 dispone que dichas instituciones deben obtener la autorización previa del BCU y que deben ajustar su actividad a las disposiciones de dicha ley, a su reglamentación y a las normas generales e instrucciones particulares que dicte el BCU.

Para otorgar la autorización, el BCU tendrá en cuenta razones de legalidad, de oportunidad y de conveniencia.

El 27 de diciembre de 2018, el BCU publicó la Circular Nº 2.316 modificando en parte la Recopilación de Normas del Sistema de Pagos, específicamente en lo vinculado a los emisores de dinero electrónico e instituciones de intermediación financiera que emiten dinero electrónico, agregando, entre otras cosas, lo referente a la habilitación para emitir dinero electrónico.

Entre los principales innovaciones se incorpora el concepto de “tecnología de pago sin contacto”, que permite realizar transacciones por proximidad con cualquier dispositivo de pago, por ejemplo: tarjetas o teléfonos celulares, utilizando el estándar internacional EMV.

(III.3.C.) Monedas digitales

Si bien en muchos países se está regulando sobre las monedas digitales, en Uruguay no hay regulación específica. No obstante, vale comentar que en las Jornadas VII de Derecho del Banco Central del Uruguay (BCU), representantes del BCU señalaron que consideran a las criptomonedas y a los *tokens* como un registro digital que carece de existencia en el mundo real y que, entre otras cosas, aspira a ser un medio de cambio. Consideran que serían como un bien mueble, inmaterial, que existe en una plataforma digital.

En relación al régimen jurídico, manifestaron, entre otras cosas, que:

i. Aplicaría el régimen de permuta por otros bienes y servicios (regulado por los artículos 1769 y siguientes del Código Civil y artículos 572 y siguientes del Código de Comercio) y de compraventa por dinero fiduciario (regulado por los artículos 1661 y siguientes del Código Civil y artículos 513 y siguientes del Código de Comercio).

ii. Se deben atender las normas de Control de Lavado de Activos y Financiamiento de Terrorismo (Ley Nº 19.574: artículos 12 y siguientes).

Debiendo además considerarse el Decreto Nº 379/2018, especialmente lo vinculado con la debida diligencia intensificada, en tanto se puede considerar que se utilizan tecnologías nuevas o en desarrollo que favorezcan el anonimato en las transacciones.

iii. La temática es competencia del BCU en tanto le corresponde, entre otras cosas: (a) velar por la eficiencia, la seguridad y la fiabilidad del Sistema Nacional de Pagos, así como por la transparencia, la competitividad del sistema y el respeto de los derechos de los clientes de las instituciones financieras que instruyan operaciones cursadas a través de dichos sistemas; (b) dictar normas generales e instrucciones particulares; y (c) vigilar el funcionamiento de las entidades que participan u operan en el Sistema Nacional de Pagos y de aquellas entidades que –sin integrar ese Sistema– pueden generar riesgos o introducirle ineficiencias, a juicio del BCU (artículos 20 y 21 de la Ley Nº 18.573).

iv. En relación a las *Initial Coin Offering (ICOs)*, entienden que quedarían alcanzadas por la Ley de Mercado de Valores, Nº 18.627, y por ende, consideran que las

empresas solicitantes de fondos deberían inscribirse como emisores de valor de oferta pública y además inscribir los valores a ofertar.

Vale tener presente que el artículo 13 de la ley Nº 18.627 define "valores" como "*los bienes o derechos transferibles, incorporados o no en un documento, que cumplan con los requisitos que establezcan las normas vigentes*", incluyendo: acciones, obligaciones negociables, mercado de futuros, opciones, cuotas de fondos de inversión, títulos valores, así como en general, todo derecho de crédito o inversión.

Considerando la amplitud de la definición legal, por Circular Nº 2.275 del 23 de enero de 2017, el BCU incorporó a la Recopilación de Normas del Mercado de Valores el artículo 3.1, definiendo que *"se considera valores aquellos bienes o derechos transferibles, emitidos en forma física o escritural y que confieren a sus titulares derechos de crédito o inversión".* A modo de ejemplo señala: acciones, bonos, certificados de depósito bancario, obligaciones negociables, contratos de futuros, opciones y derivados en general, cuota partes de fondos de inversión, títulos de deuda, certificados de participación o títulos mixtos de fideicomisos financieros, vales, conformes, pagarés, letras de cambios, cheques, notas de crédito hipotecarias, entre otros títulos valores, certificados de depósito y *warrants*.

No hay regulación específica sobre los ICOs, ni sobre otras formas de financiación colectiva.

(III.3.D.) Modalidad de financiación colectiva

Las plataformas digitales de financiación colectiva permiten visualizar y conectar la capacidad excedentaria de unos, con la demanda de financiación de otros.

Tiene tres bases fundamentales. Por un lado permite promover, mejorar y facilitar el acceso al crédito que necesitan personas jurídicas y físicas, otorgando más opciones con menores costos. Por otro lado, mejora el rendimiento de los ahorros de personas jurídicas y físicas, creando nuevas opciones de ahorro para todos los pequeños y medianos ahorristas; y finalmente, favorece la transparencia, la inclusión, la seguridad, la innovación y el desarrollo.

Si bien en la mayoría de los países este tipo de actividades –a través de plataformas electrónicas– se comenzó a desarrollar hace más de diez años, en Uruguay comenzó hace relativamente pocos años –años 2015 y 2016–.

Como planteábamos anteriormente, considerando que en muchos supuestos las normativas fueron pensadas para realidades diferentes, con la utilización de plataformas electrónicas para prestar servicios, en muchos supuestos se genera inseguridad jurídica respecto al alcance de la regulación vigente.

Un claro ejemplo se planteó en el año 2017. El BCU, tras observar el esquema de negocios de una plataforma que brindaba este tipo de servicios, señaló la importancia de diferenciar entre la actividad de intermediación financiera, la cual requiere autorización del Poder Ejecutivo, y la mediación; y señaló la necesidad de regular este tipo de servicios.

La intermediación comprende: i. operaciones pasivas: el intermediario se hace dueño de los recursos económicos ajenos; y ii. operaciones activas: el intermediario transfiere a terceros los recursos financieros. Mientras que en la mediación, simplemente se pone en contacto a dos contratantes o asume una obligación eventual o accesoria. Los recursos son ajenos al mediador. La diferencia entre ambas actividades, no es el origen de los fondos, sino la participación. El intermediario hace propios los fondos, no así el mediador.

En este sentido, en diciembre de 2017, la Superintendencia de Servicios Financieros (SSF) publicó las bases y lineamientos para una futura regulación de empresas administradoras de plataformas para préstamos entre personas. Señaló que existen en el mercado local diversas empresas operando plataformas cuyos modelos de negocios se inspiran en mecanismos de desarrollo reciente en otros mercados, los cuales se conocen de diferentes formas, como ser: "préstamos entre personas", "préstamos entre particulares o entre particulares y empresas", "*peer-to-peer lending", "crowdeling*", entre otros. No debiendo confundirse con préstamos de otros tipos, como pueden ser "*crowdfunding*", "financiación colectiva" o "financiación masiva".

Al respecto señalan que la operación de sistemas de préstamos entre personas, en la medida en que el administrador se limita a aproximar a las partes en negocios de préstamos de dinero, sin asumir obligación o riesgo alguno, implica una actividad bajo control del BCU en virtud de lo establecido en el numeral II) del artículo 37 de su Carta Orgánica (Ley Nº 16.696), en cual dispone que la SSF reglamentará y controlará las actividades de aquellas entidades que:

"II) Se limiten a aproximar o asesorar a las partes en negocios de carácter financiero sin asumir obligación o riesgo alguno. (...)

La reglamentación y fiscalización de las entidades comprendidas en los numerales I y II del inciso precedente se limitarán a otorgar la adecuada información a los consumidores, procurar la protección de los mismos respecto a las prácticas abusivas y la prevención en el lavado de activos y financiamiento del terrorismo."

Pese a que la normativa expresamente limita el alcance de la regulación, a mediados de 2018, la SSF publicó el proyecto de reglamentación de la actividad de las empresas que administran plataformas para préstamos entre personas, yendo más allá de lo que la norma prevé; y finalmente el 23 de noviembre de 2018, el BCU aprobó la Circular Nº 2.307.

Como surge de Versión Taquigráfica del 17 de diciembre de 2018 de la Comisión Especial de Innovación, Ciencia y Tecnología de la Cámara de Representantes, en la que se trató la temática y en la que participaron también representantes del BCU, se planteó que la circular causó muchos daños en la industria, que muchas plataformas dejaron de operar y migraron a otros países. Asimismo, se señaló que "*Los puntos más críticos serían: primero, no permitir manejar los fondos por parte de las empresas administradoras, que se entiende esencial poder hacerlo; segundo, no permitir el emparejamiento automático con reglas preaprobadas, es decir, montos, plazos, tasas y riesgo; se dice (...) que habilitar el uso de algoritmos es la tendencia mundial, sobre todo, en el corazón de estos negocios; tercero, la habilitación a la plataforma para invertir fondos propios sin que se le apliquen los límites dispuestos; cuarto, los límites a la inversión, que no permitirían la escalabilidad necesaria; quinto, que se plantee la inconveniencia de que el documento de adeudo no deba ser a la orden, y sexto, la confidencialidad, sobre la cual no entiendo el fundamento de obligar a develar la identidad de las partes que contratan."*

Entre los puntos más críticos de la reglamentación, se plantearon los siguientes:

1. la necesidad de establecer modalidades específicas que permitieran a las empresas administrar los movimientos de los fondos, manteniendo la ajenidad de los mismos;

2. que la tendencia es utilizar la automatización de procesos que permiten hacer emparejamientos automáticos entre oferta y demanda, dando garantías y seguridad, pero que con la reglamentación aprobada no se podrían hacer;

3. se propuso diferenciar entre los tipos de inversores, calificados y no calificados, estableciendo límites diversos para uno y otro, así como requisitos de contralor que se ajusten a cada caso. Se establecieron límites que no permiten la escalabilidad;

4. se establecen formalidades para la documentación, como que sean nominativos, no a la orden y que deban ser celebrados por medios físicos, lo cual deja de lado lo establecido en el Decreto-Ley 14.701 y en el artículo 3 de la Ley 18.600 que establece, entre otras cosas, el principio de equivalencia funcional, es decir: que todos aquellos actos o negocios jurídicos realizados electrónicamente, tendrán el mismo valor que si se realizarán por medios físicos;

5. que los socios de las plataformas solo pueden ser personas físicas, lo cual limita poder conseguir y captar inversiones, afectando la escalabilidad, así como las posibilidades de desarrollo de las empresas.

Los representantes de BCU se manifestaron ante la Comisión Especial de Innovación, Ciencia y Tecnología de la Cámara de Representantes, haciendo énfasis en la importancia de mitigar los riesgos que puede haber para el usuario del sistema financiero, como ser: lavado de activos, financiamiento de terrorismo, ciberseguridad, seguridad en la información y fraudes. Además, destacaron la importancia de contemplar, en el diseño de la regulación, un equilibrio entre mitigar esos riesgos y desarrollar el mercado del sistema financiero y del sistema de pagos, donde la *Fintech* se ha ido constituyendo en un actor cada vez más relevante.

Por otra parte, en el año 2019 se aprobó la Ley N° 19.820 sobre ¨*Promoción de emprendimientos*", donde se modifica el artículo 3° de la Ley N° 18.627, de 2 de diciembre de 2009, sobre registro de valores, que lo lleva la Superintendencia de Servicios Financieros, indicando que: *"Los emisores y las emisiones realizadas a través de plataformas de financiación colectiva se inscribirán en una sección específica del Registro y lo harán a través de las instituciones que administran dichas plataformas, conforme el régimen establecido en el artículo 93 bis de la presente ley. La Superintendencia de Servicios Financieros determinará la información que las*

instituciones administradoras le deberán suministrar para su incorporación a la referida sección del Registro".

Además, se agregó a la Ley Nº 18.627, el artículo 93 BIS, el cual establece que[452]:

"*Las plataformas de financiamiento colectivo son mercados de negociación de valores de oferta pública abiertos a la participación directa de los inversores y reservados a emisiones de monto reducido. El Banco Central del Uruguay establecerá los límites máximos de emisión por emisor así como definirá el concepto de inversor pequeño y los límites máximos de participación de dicha categoría de inversores en cada emisión."*

"Las instituciones que administren plataformas de financiamiento colectivo requerirán para funcionar autorización previa de la Superintendencia de Servicios Financieros, para el otorgamiento de la cual serán valoradas razones de legalidad, oportunidad y conveniencia..."

"Los emisores y las emisiones negociadas en plataformas de financiación colectiva se inscribirán ante la misma institución administradora, en las condiciones que establezca la regulación del Banco Central del Uruguay. La administradora oficiará como representante de los tenedores, como agente de pago y como entidad registrante de los valores, y será responsable de divulgar la información periódica del emisor y de la emisión exigidas por la reglamentación. Asimismo, la administradora deberá registrar los emisores y las emisiones en una sección específica que incorporará el Registro de Mercado de Valores, cumpliendo los requisitos que determine la Superintendencia de Servicios Financieros."

Además se prevé determinados límites: *"No podrán efectuar emisiones en estas plataformas las personas jurídicas cuyas ventas anuales superen el valor máximo que establezca la Superintendencia de Servicios Financieros."*

Se prevé la reglamentación por parte del BCU la cual será de gran importancia a los efectos de la implementación. En setiembre del corriente el BCU compartió el proyecto para regular estas plataformas buscando equilibrio entre impulsar el financiamiento para los emprendedores, al tiempo que proteger a los inversores.

[452] Ibídem.

IV. Consideraciones finales

Las plataformas digitales ofrecen un mundo de oportunidades y de beneficios para los usuarios; sin duda hay que identificar los riesgos y trabajar sobre los mismos para mitigarlos, mas la innovación es esencial para el desarrollo económico y social.

El diálogo entre los diversos actores es fundamental, los cambios se producen cada vez más rápido y la regulación juega un rol muy importante, siendo básico que sea adecuada, que se revise y actualice de ser necesario, a fin de que atienda la realidad del sector, que no lo limite sin reales argumentos, al tiempo que proteja a los usuarios y otorgue seguridad jurídica para facilitar la innovación, el desarrollo y atraer inversiones.

Una buena práctica que se está implementando en derecho comparado es el método "caja de arena" o "*Sandbox*", que permite realizar ensayos reales entre las empresas y los reguladores, en entornos controlados, por un plazo determinado. Generan un ecosistema similar al mercado real, donde las empresas, los reguladores y consumidores interactúan, aprenden en conjunto, identifican los puntos y las garantías que hay que atender.

No podemos pretender responder adecuadamente a las nuevas realidades, con modelos y soluciones pensadas para supuestos diferentes. Tenemos que alcanzar soluciones más innovadoras y más eficientes, que nos permitan desarrollar y crear empleo, captar talento e inversiones.

Hay que empoderar a las personas, protegerlas, así como promover el desarrollo de las redes y de los servicios y aplicaciones digitales, buscando que todos tengan acceso. Fomentar la innovación y la defensa de la competencia es fundamental, así como dejar atrás las regulación de marco rígido preconcebido, para empezar a trabajar en la nueva realidad dinámica y de cambio permanente.

Las TIC atraviesan a todos los sectores de la economía y como tal la regulación debe adquirir un carácter colaborativo, siendo fundamental una articulación entre los diversos actores. Se necesitan reglas claras, lo cual no debe confundirse con regulaciones rígidas que rápidamente quedan desactualizadas y terminan limitando. Hay que dar marcos que promuevan e impulsen, dando seguridad sin limitar.

En definitiva, la regulación un factor que facilitará y diferenciará a los países. Aquellos que entiendan, atiendan y promuevan la nueva realidad, con una visión cabal, desarrollarán mejor el ecosistema generando más oportunidades para todos.

Es esencial responder de una manera más inteligente, adecuada, evitando errores, ateniendo la necesidad y la realidad, de forma proporcional.

Para lo cual debemos: (i) Aprender de las experiencias que ya tienen otros países, algunos tienen más camino transitado en la temática. (ii) Trabajar en conjunto, entender y dialogar entre los diversos actores del sector. (iii) Medir, controlar, así como revisar periódicamente las soluciones adoptadas.

El marco jurídico de España viene desarrollándose y actualizándose desde hace más de quince años. En Uruguay recientemente se aprobó una Ley para promover el emprendedurismo y la financiación, hay un proyecto de reglamentación pero aún no se ha aprobado.

Si bien Uruguay venía más avanzando en los aspectos tributarios, España recientemente aprobó una ley específica para los servicios digitales, la cual entrará en vigencia en enero 2021.

La regulación española recibió críticas por no adaptarse a la realidad y a las necesidades, lo cual llevó a que muchas empresas se instalen en países más amigables y que ofrecieran reglas más claras, como Inglaterra. Uruguay debería aprender de la experiencia de España, tanto de los aspectos positivos como de los negativos.

La regulación debe ser más inteligente, flexible, realizada en conjunto, siendo fundamental la revisión periódica para no afectar la innovación, el desarrollo, la investigación y la inversión. Los cambios están ocurriendo muy de prisa y los países que mejor respondan a la nueva realidad digital generarán más oportunidades para sus ciudadanos.

CAPÍTULO VII: LAS TIC Y LOS DERECHOS FUNDAMENTALES

I. Introducción

El gran desarrollo que han tenido las nuevas tecnologías y las telecomunicaciones, ha generado grandes cambios sociales y económicos. Todos los aspectos de nuestras vidas se han visto sumergidos en Internet y la tendencia se profundiza cada vez más.

Se ha facilitado la creación y universalización de nuevos servicios y aplicaciones digitales, que atienden diversas necesidades de la sociedad, que se brindan sobre plataformas electrónicas, como pueden ser: Twitter y Facebook; y que han generado un ecosistema digital que: borra fronteras, refleja que vivimos en una comunidad internacional, ofrece más acceso, empodera a las personas y genera múltiples oportunidades.

No obstante, el ecosistema digital tiene muchos riesgos y retos, principalmente en relación con los derechos humanos, lo cual obliga a las autoridades a enfrentar la necesidad de desarrollar soluciones internacionales que permitan realizar plenamente los derechos y libertades reconocidos en la Declaración Universal de los Derechos Humanos (DUDH), así como en otros instrumentos internacionales.

La DUDH proclamó un estándar común para el logro de todas las personas y naciones. Estableció los derechos humanos fundamentales que deben ser protegidos universalmente por el Estado de Derecho y que deben ser promovidos para asegurar su efectividad, en la medida en que son esenciales para lograr la libertad, la justicia y la paz en el mundo.

Su proclamación se presenta como un "*ideal común por el que todos los pueblos y naciones deben esforzarse, a fin de que tanto los individuos como las instituciones, inspirándose constantemente en ella, promuevan, mediante la enseñanza y la educación, el respeto a estos derechos y libertades, y aseguren, por medidas progresivas de carácter nacional e internacional, su reconocimiento y aplicación universales y efectivos, tanto entre los pueblos de los Estados Miembros como entre los de los territorios colocados bajo su jurisdicción*"[453].

453 Declaración Universal de Derechos Humanos. URL: https://www.un.org/es/universal-declaration-human-rights/ Consultado el 20 de febrero de 2019.

La Declaración está formada por 30 artículos, estableciendo entre otras cosas:

Artículo 1: *"Todos los seres humanos nacen libres e iguales en dignidad y derechos y, dotados como están de razón y conciencia, deben comportarse fraternalmente los unos con los otros".*

Artículo 12: *"Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques".*

Artículo 18: *"Toda persona tiene derecho a la libertad de pensamiento, de conciencia y de religión; este derecho incluye la libertad de cambiar de religión o de creencia, así como la libertad de manifestar su religión o su creencia, individual y colectivamente, tanto en público como en privado, por la enseñanza, la práctica, el culto y la observancia".*

Artículo 19: *"Todo individuo tiene derecho a la libertad de opinión y de expresión; este derecho incluye el de no ser molestado a causa de sus opiniones, el de investigar y recibir informaciones y opiniones, y el de difundirlas, sin limitación de fronteras, por cualquier medio de expresión".*

Artículo 27: *"1. Toda persona tiene derecho a tomar parte libremente en la vida cultural de la comunidad, a gozar de las artes y a participar en el progreso científico y en los beneficios que de él resulten.*

2. Toda persona tiene derecho a la protección de los intereses morales y materiales que le correspondan por razón de las producciones científicas, literarias o artísticas de que sea autora."

En esta línea, el Preámbulo de la Constitución Española señala que *"La Nación española, deseando establecer la justicia, la libertad y la seguridad y promover el bien de cuantos la integran, en uso de su soberanía, proclama su voluntad de:*

Garantizar la convivencia democrática dentro de la Constitución y de las leyes conforme a un orden económico y social justo.

Consolidar un Estado de Derecho que asegure el imperio de la ley como expresión de la voluntad popular.

Proteger a todos los españoles y pueblos de España en el ejercicio de los derechos humanos, sus culturas y tradiciones, lenguas e instituciones.

Promover el progreso de la cultura y de la economía para asegurar a todos una digna calidad de vida.

Establecer una sociedad democrática avanzada, y

Colaborar en el fortalecimiento de unas relaciones pacíficas y de eficaz cooperación entre todos los pueblos de la Tierra".

Y, entre otras bases, dispone que:

"1. La dignidad de la persona, los derechos inviolables que le son inherentes, el libre desarrollo de la personalidad, el respeto a la ley y a los derechos de los demás son fundamento del orden político y de la paz social.

2. Las normas relativas a los derechos fundamentales y a las libertades que la Constitución reconoce se interpretarán de conformidad con la Declaración Universal de Derechos Humanos y los tratados y acuerdos internacionales sobre las mismas materias ratificados por España"[454].

"Toda persona tiene derecho a la libertad y a la seguridad"[455].

"Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen"[456].

"Se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial"[457].

"La ley limitará 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"[458].

"El reconocimiento y la protección de los derechos a[459]*:*

A expresar y difundir libremente los pensamientos, ideas y opiniones mediante la palabra, el escrito o cualquier otro medio de reproducción.

A la producción y creación literaria, artística, científica y técnica.

[454] Artículo 10 de la Constitución Española.
[455] Artículo 17 de la Constitución Española.
[456] Artículo 18.1 de la Constitución Española.
[457] Artículo 18.3 de la Constitución Española.
[458] Artículo 18.4 de la Constitución Española.
[459] Artículo 20 de la Constitución Española.

A la libertad de cátedra.

A comunicar o recibir libremente información veraz por cualquier medio de difusión. La ley regulará el derecho a la cláusula de conciencia y al secreto profesional en el ejercicio de estas libertades.

4. Estas libertades tienen su límite en el respeto a los derechos reconocidos en este Título, en los preceptos de las leyes que lo desarrollen y, especialmente, en el derecho al honor, a la intimidad, a la propia imagen y a la protección de la juventud y de la infancia".

"Todos tienen el derecho a la educación. Se reconoce la libertad de enseñanza"[460].

"1. Los poderes públicos promoverán las condiciones favorables para el progreso social y económico y para una distribución de la renta regional y personal más equitativa, en el marco de una política de estabilidad económica. De manera especial realizarán una política orientada al pleno empleo.

2. Asimismo, los poderes públicos fomentarán una política que garantice la formación y readaptación profesionales; velarán por la seguridad e higiene en el trabajo y garantizarán el descanso necesario, mediante la limitación de la jornada laboral, las vacaciones periódicas retribuidas y la promoción de centros adecuados"[461].

"2. Los poderes públicos promoverán la ciencia y la investigación científica y técnica en beneficio del interés general"[462].

"1. Los poderes públicos garantizarán la defensa de los consumidores y usuarios, protegiendo, mediante procedimientos eficaces (...).

2. Los poderes públicos promoverán la información y la educación de los consumidores y usuarios..."[463].

Los derechos señalados, reconocidos en la Declaración y en la Constitucional española, son a mero título enunciativo, siendo muestra de algunos de los derechos que

[460] Artículo 27 de la Constitución Española.
[461] Artículo 40 de la Constitución Española.
[462] Artículo 44.2 de la Constitución Española.
[463] Artículo 51 de la Constitución Española.

todas las personas tenemos, independientemente de que estemos en el mundo digital o en el mundo tradicional.

En este sentido, si bien el ecosistema digital permite innovar y alcanzar soluciones que facilitan la vida de todos, con impacto positivo en la sociedad, no se puede dejar de lado que un mal uso de las herramientas, puede afectar el interés general, así como vulnerar derechos fundamentales de las personas.

En este entorno, como se reconoció en la Cumbre Mundial de la Sociedad de la Información (CMSI) del año 2015, entre los principales retos se destacan:

i. Proteger a todos los derechos humanos, garantizando que se respeten tanto en línea (*online*) como fuera de línea (*offline*).

ii. Integrar la perspectiva de igualdad entre hombres y mujeres, buscando: empoderar a las mujeres, su plena participación, así como la igualdad en todas las esferas de la sociedad y en los procesos decisorios.

iii. Reducir la brecha digital. Ampliar el acceso a las Tecnologías de la Información y las Comunicaciones (TIC) y conectar a la población mundial, para lo cual es necesario mejorar la gestión y la utilización del espectro radioeléctrico, así como facilitar la construcción e implantación de redes de telecomunicaciones.

iv. Aumentar el acceso a la información, a la educación y al conocimiento para todos. Siendo necesario que todas las personas tengan los conocimientos y los medios básicos para participar en la sociedad de la información.

v. Garantizar el pleno derecho de todas las personas a expresarse, a crear y a difundir sus obras y contenidos.

vi. Respetar la diversidad humana en todas sus formas, la cultura, las lenguas, tradiciones, creencias y religiones.

vii. Generar confianza en la utilización de las TIC, siendo fundamental aumentar la seguridad y la privacidad en la red.

viii. Concientizar la dimensión ética de la utilización de las TIC y propiciar un diálogo interdisciplinario.

Los retos y objetivos son muchos, mas lo esencial es identificarlos y trabajar sobre los mismos, junto con los diversos actores de la sociedad, a fin de que Internet y el

ecosistema digital se pueda seguir desarrollando, al tiempo que se garanticen los derechos fundamentales de todos.

En este sentido, a los efectos del presente trabajo, interesa analizar principalmente los derechos vinculados a: la privacidad y la protección de los datos personales, la expresión y el acceso a la información, los derechos de autor, y la seguridad en el mundo digital; por la importancia que tienen por sí mismos, así como por el rol que desempeñan para el desarrollo de otros derechos y de la nueva era digital.

II. Privacidad y datos personales (DP)[464]

Estamos ante un nuevo mundo de oportunidades, en el que, entre otras cosas: gran parte de la población mundial está hiperconectada, los diversos aspectos de nuestras vidas pasan a estar digitalizados, las nuevas tecnologías disrumpen y transforman, generando grandes cambios, a gran velocidad.

Con la transformación digital, pasamos de los átomos a los bits, lo cual junto con más capacidad de almacenamiento y de procesamiento, sumado a la universalización del acceso a las telecomunicaciones y a la aplicación conjunta de diversas tecnologías –como puede ser la inteligencia artificial, el big data, el aprendizaje automático, la robótica, el almacenamiento en la nube, la blockchain, por mencionar algunos de los principales drivers-; la velocidad de los cambios se va a acelerar cada vez más, y los datos, la información, juegan un rol fundamental.

Con la digitalización de los datos, tenemos cada vez más información, la cual tiene mucho valor, es un gran producto alrededor del cual se han generado diversas formas de comercialización, en tanto algunas empresas recopilan datos y actúan como asesoras de otras, al tiempo que las organizaciones los pueden utilizar para conocer y captar más público, generando fidelización, diferenciándose y creando grandes ventajas competitivas.

Con la digitalización de la información y todos los datos que hay en línea, se han desarrollado diversos programas y tecnologías que nos permiten almacenar, procesar y

464 Véase nuestro trabajado, ARAMENDÍA, MERCEDES, "La protección de los datos personales es esencial para el desarrollo del mundo digital. Primeras aproximaciones al nuevo reglamento general de datos de la Unión Europea" en *Estudios de Información Pública y Datos Personales,* Tomo III, Universidad de Montevideo, 2019, pp. 387 y ss.

analizar toda la información a gran velocidad, de manera simple, económica y automatizada, pudiendo ver, predecir y tomar decisiones más informadas en tiempo real.

Sin duda lo anterior tiene muchos beneficios, pero también implica muchos riesgos. Hay temas de seguridad, de categorizar los datos -las computadoras no tienen, por lo menos aún no la mayoría, la habilidad para determinar la naturaleza o la sensibilidad de la información-, debiendo buscar la mejor forma de proteger los derechos fundamentales de las personas, como su privacidad e intimidad.

El Diccionario de la Real Academia Española define ¨privacidad¨ como: *¨1. Cualidad de privado. 2. Ámbito de la vida privada que se tiene derecho a proteger de cualquier información'*[465]*;* y define ¨intimidad¨ como *¨2. Zona espiritual íntima y reservada de una persona o de un grupo, especialmente de una familia¨*[466].

Sobre estos conceptos, resulta interesante señalar que la privacidad suele verse como un concepto más amplio que la intimidad, en tanto la intimidad se presenta más como la *¨esfera en que se desarrollan las facetas más singularmente reservadas de la vida de la persona -el domicilio donde realiza su vida cotidiana, las comunicaciones en las que expresa sus sentimientos, por ejemplo-, la privacidad constituye un conjunto, más amplio, más global, de facetas de su personalidad que, aisladamente consideradas, pueden carecer de significación intrínseca pero que, coherentemente enlazadas entre sí, arrojan como precipitado un retrato de la personalidad del individuo que éste tiene derecho a mantener reservado*[467]*¨*.

Con el uso de la tecnología, podemos transmitir muchos datos de las personas, lo cual junto con la gran capacidad de almacenamiento y de procesamiento de datos, nos permiten recopilar y trabajar sobre grandiosos volúmenes de información. Lo anterior puede ser muy beneficioso para la sociedad, pero es fundamental que se haga adecuadamente, que los datos personales no se traten automatizadamente, lo cual también implica que se pueden transmitir fácilmente, en tanto un mal uso de las herramientas puede vulnerar la privacidad y la intimidad de las personas, así como la confidencialidad y la seguridad.

---

[465] Diccionario de la Real Academia Española, definición de Privacidad. URL: https://dle.rae.es/privacidad Consultado el 30 de enero de 2019.

[466] Diccionario de la Real Academia Española, definición de Intimidad. URL: https://dle.rae.es/intimidad Consultado el 30 de enero de 2019.

[467] Exposición de Motivos de la Ley Orgánica 5/992 de España, actualmente derogada, que regulaba el tratamiento automatizado de los datos de carácter personal.

En esta nueva realidad, la privacidad de las personas toma cada vez mayor exposición y relevancia. Los datos personales son parte de la intimidad de las personas, de su dignidad, y su protección es un derecho fundamental reconocido y protegido por diversos instrumentos internacionales, como ser: artículo 12 de la DUDH[468], artículo 17 del Pacto Internacional de Derechos Civil y Políticos[469], artículo 11 de la Convención Americana sobre Derechos Humanos[470], el artículo 8 de Convenio Europeo de Derechos Humanos (CEDH)[471], el artículo 16.1 del Tratado de Funcionamiento de la Unión Europea[472], y la cuarta enmienda de la Constitución de los Estados Unidos[473].

En España, la Protección de Datos de Carácter Personal es un derecho fundamental protegido por el artículo 18.4[474] de la Constitución y está regulada por la Ley Orgánica N° 3/2018 (LOPDGDD) de 6 de diciembre de 2018. No obstante, a nivel legislativo, este derecho fundamental de protección de las personas físicas en relación con el tratamiento de datos personales tuvo su origen en la Ley Orgánica 5/1992,

468 Artículo 12 de la DHDU: *"Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques."*

469 Artículo 17 del Pacto Internacional de Derechos Civiles y Políticos: "1. *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. 2. Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques."*

470 Artículo 11 de la Convención Americana sobre Derechos Humanos: "1. *Toda persona tiene derecho al respeto de su honra y al reconocimiento de su dignidad. 2. Nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada, en la de su familia, en su domicilio o en su correspondencia, ni de ataques ilegales a su honra o reputación. 3. Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques."*

471 Artículo 8 del CEDH: "1. *Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia. 2. No podrá haber injerencia de la autoridad pública en el ejercicio de este derecho, sino en tanto en cuanto esta injerencia esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención del delito, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás."*

472 Artículo 16.1 del TFUE: *"1. Toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan."*

473 Amendment IV: *"The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized".*

474 Artículo 18 de la Constitución de España: "*1. Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen. 2. El domicilio es inviolable. Ninguna entrada o registro podrá hacerse en él sin consentimiento del titular o resolución judicial, salvo en caso de flagrante delito. 3. Se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial. 4. La ley limitará 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."*

reguladora del tratamiento automatizado de datos personales, posteriormente reemplazada por la Ley Orgánica 15/1999, de protección de datos personales, que traspuso la Directiva 95/46/CE del Parlamento Europeo y del Consejo, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

En Uruguay, el artículo 28 de la Constitución prevé que *"los papeles de los particulares y su correspondencia epistolar, telegráfica o de cualquier otra especie, son inviolables, y nunca podrá hacerse su registro, examen o interceptación sino conforme a las leyes que se establecieren por razones de interés general",* y además, como surge de la Ley Nº 18.331, la protección de los datos personales se considera un derecho humano, inherente a la personalidad humana, comprendido en el artículo 72 de la Constitución[475]. Al respecto, cabe destacar que –como enseña el profesor Esteva– el artículo 72 es abierto, lo que habilita la integración, tomando especial importancia –como señala el profesor Cajarville– los principios generales de derecho y los Tratados internacionales ratificados por Uruguay en materia de Derechos Humanos.

Como surge de la publicación "*El derecho a la privacidad en la era digital*[476]" de Naciones Unidas del 24 de marzo de 2015: *"el rápido ritmo del desarrollo tecnológico permite a las personas de todo el mundo utilizar la nueva tecnología de la información y las comunicaciones y, al mismo tiempo, incrementa la capacidad de los gobiernos, las empresas y las personas de llevar a cabo actividades de vigilancia, interceptación y recopilación de datos, lo que podría constituir una violación o una transgresión de los derechos humanos, en particular del derecho a la privacidad, establecido en el artículo 12 de la Declaración Universal de Derechos Humanos y el artículo 17 del Pacto Internacional de Derechos Civiles y Políticos, y que, por lo tanto, esta cuestión suscita cada vez más preocupación*". *"...si bien los metadatos pueden aportar beneficios, algunos tipos de metadatos, tomados en conjunto, pueden revelar información personal y pueden dar indicación del comportamiento, las relaciones sociales, las preferencias privadas y la identidad de una persona"(...) "los Estados deben respetar las*

475 Artículo 72 de la Constitución. *La enumeración de derechos, deberes y garantías hecha por la Constitución, no excluye los otros que son inherentes a la personalidad humana o se derivan de la forma republicana de gobierno.*

476 Naciones Unidas: "El derecho a la privacidad en la era digital". URL: http://ap.ohchr.org/documents/S/HRC/d_res_dec/A_HRC_28_L27.pdf. Consultado el 11 de marzo de 2019.

obligaciones internacionales de derechos humanos en lo referente al derecho a la privacidad cuando intercepten las comunicaciones digitales de las personas o reúnan datos personales y cuando exijan a terceros, incluidas las empresas privadas, la divulgación de datos personales".

Asimismo, además de lo referente a la vigilancia y a la interceptación, el desarrollo de la tecnología, como pueden ser la inteligencia artificial, el Internet de las cosas, *big data,* el almacenamiento en la nube, *Blockchain*, entre otros ejemplos, recopilan y se alimentan de datos que pueden utilizarse para diversos fines. Tienen muchos beneficios para la sociedad, pero pueden conllevar riesgos para la privacidad de las personas si no se toman las medidas o cautelas necesarias.

La inteligencia artificial tiene como objetivo fundamental la automatización de comportamientos, razonar, recabar, tratar y procesar información, entre otros ejemplos. Engloba muchos conceptos, como ser: la informática cognitiva (algoritmos capaces de razonar y comprender), el aprendizaje automático (algoritmos capaces de enseñarse a sí mismos), la inteligencia aumentada (colaboración entre personas y máquinas) o la robótica integrada con inteligencia artificial. Tiene muchas aplicaciones, como ser asistentes virtuales, publicación automática de noticias, programas de traducción, filtrado de contenidos, negociaciones financieras, investigaciones jurídicas, entre otros múltiples ejemplos[477]. Se nutre de datos, para lo cual requieren mucha cantidad de información, de buena calidad.

Internet de las cosas permite, entre otras utilidades, que las cosas que usamos todos los días, desde un instrumento de cocina hasta los juegos de los niños, puedan brindar información útil a través de Internet –como por ejemplo el comportamiento de las personas que utilizan dichos dispositivos, en qué modalidades se utilizan más, cómo es el tipo de uso, etc.–, todo lo cual permite realizar un gran análisis, conocer tendencias y acelerar la toma de decisiones.[478]

El big data –junto con la inteligencia artificial y el Internet de las cosas– permite recolectar, combinar y analizar a gran velocidad, cuantiosas cantidades de datos, facilitando conocer tendencias de valor, innovar, optimar la productividad, mejorar las

477 Dictamen del Comité Económico y Social Europeo. URL: https://eur-lex.europa.eu/legal-content/ES/ALL/?uri=uriserv:OJ.C_.2017.288.01.0001.01.SPA. Consultado el 20 de febrero de 2019.
478 Ibídem, pp. 34.

acciones públicas y la participación social. Asimismo, modifica la forma de entender y organizar la sociedad, pudiendo tomar decisiones más informadas[479].

Se destaca por las tres "v": volumen, variedad y velocidad. [480]

En relación al volumen, debemos pensar en una cantidad tal de información que no pueden ser procesados o analizados con las herramientas tradicionales, en tanto superan sus límites y capacidades. Respecto a la variedad, hay que imaginar datos que derivan de diversas fuentes, por ejemplo: de GPS, teléfonos celulares, medidores electrónicos, etc., que pueden brindar diversa información: movimiento, ubicación, temperatura, etc. Finalmente, vinculado a la velocidad, cuanto más rápido se puedan procesar y analizar estos datos, más expeditivamente se va a poder obtener información correcta, identificar oportunidades y actuar en consecuencia.[481]

Para atender esta realidad, se han desarrollado infraestructuras, tecnologías y servicios para procesar enormes cantidad de datos estructurados, no estructurados o semiestructurados (por ejemplo: mensajes en redes sociales, señales de móvil, audios, sensores, imágenes digitales, datos de formularios, e-Mails, datos de encuestas, etc.) que pueden provenir de diversos instrumentos, como ser: sensores, micrófonos, cámaras, etc.[482].

Haciendo uso de estas herramientas, se modifica la forma de entender y de explorar. Antes nos debíamos guiar por hipótesis que intentábamos validar; en el futuro nuestra comprensión estará impulsada más por el análisis de abundantes datos en vez de por hipótesis.[483] Los datos se convirtieron en un insumo esencial para los negocios, que permite realizar enormes ahorros económicos, modificar o ajustar los servicios y

---

479 Consejo de Europa: "Guidelines on the protection of individuals with regard to the processing of personal data un a world of Big Data", publicado en URL: www.coe.int/data-protection Consultado el 15 de setiembre de 2019.

480 PUYOL MONTERO, JAVIER: *Aproximación jurídica y económica al big data*, Tirant lo Blanch, Valencia, 2015, pp. 17.

481 Cfr.: IBM. ¿Qué es Big Data? ¿Qué es Big Data? ¿Qué es Big Data?. IBM developerWorks.https://www.ibm.com/developerworks/ssa/local/im/que-es-big-data, citado por PUYOL MONTERO, JAVIEER, "Big Data" en *El derecho de Internet*, Atelier, Libros Jurídicos, año 2016, pp. 69 y ss.

482 Cfr. La moda del Big Data: ¿En qué consiste en realidad? El Economista.es http://www.eleconomista.es/interstitial/volver/240878542/tecnología/noticias/5578707/02/12/La-moda-del-Big-Data-En-que-consiste-en-realidad.html#Kku8R0DYyeF7LGSI, citado por Javier PUYOL MONTERO en "Big Data", obra citada, pp. 70.

483 Ibídem, pp. 70.

productos, buscando crear más valor[484]. Pueden reutilizarse, convirtiéndose en una fuente de innovación y de nuevos servicios; y como dicen: "los datos pueden revelar secretos a aquellos con la humildad, la voluntad y la necesidad de escuchar"[485]. Como dice Jeff Jonas, experto de IBM de *big-data*, "tienes que dejar que el dato te hable a ti"[486].

Lo anterior conlleva múltiples beneficios para la sociedad, mas en base a lo establecido en las *¨Directrices sobre la protección de las personas con respecto al procesamiento de datos personales en un mundo de big data¨*[487] del Consejo de Europa, destaco los siguientes lineamientos:

Usar los DP de forma ética y consciente, equilibrando los intereses, protegiendo los derechos humanos y las libertades individuales.

Garantizar la protección de los individuos ante el procesamiento de DP, considerando el impacto legal, social y ético del uso del big data, teniendo en cuenta el derecho a la igualdad y de no discriminación.

Mitigar los riesgos con soluciones desde el diseño, controlar y evaluar las soluciones provistas.

Limitar el procesamiento para el fin legítimo que fueron recabados, poniendo a disposición los resultados del proceso, respetando la información confidencial, reservada o secreta.

El consentimiento debe ser libre, informado e inequívoco.

Anonimizar los DP de manera que no se pueda identificar o reidentificar a las personas.

Garantizar que no haya intervención humana en el proceso de toma de decisiones.

Ayudar a las personas a comprender las implicancias del uso de los DP en el big data.

---

484 MAYER-SCHÖNBERGER, VIKTOR Y CUKIER, KENNETH, *Big Data - A Revolution that will transform how we live, work and think*, John Murray. Londres. 2013, pp. 5 y ss.

485 MAYER-SCHÖNBERGER, VIKTOR Y CUKIER, KENNETH, obra citada, pp. 5.

486 Traducción propia: "Jeff Jonas says you need to let the data «speak to you»" en MAYER-SCHÖNBERGER, Viktor y CUKIER, Kenneth, obra citada, pp. 19.

487 Idem. URL: https://rm.coe.int/16806ebe7a Consultado el 15 de setiembre de 2019.

El almacenamiento en la nube "*utiliza una red de servidores remotos alojados en Internet para almacenar, gestionar y procesar datos, en lugar de hacerlo con un servidor local o una computadora personal. Se refiere a una infraestructura de Internet bajo demanda y de autoservicio que permite al usuario acceder a recursos informáticos en cualquier momento y desde cualquier sitio. No se trata de una nueva tecnología sino de un nuevo modelo para suministrar recursos informáticos.*[488] *Entre los ejemplos más comunes de aplicaciones basadas en la nube se encuentran Dropbox y Google Docs"*[489].

Blockchain, o cadena de bloques, presenta múltiples beneficios y características que conllevan desafíos para la adecuada protección de los datos personales. Principalmente por su inmutabilidad y por la descentralización, lo cual implica que: (i) no se pueden modificar ni eliminar los datos, lo cual puede impactar directamente en los derechos de los titulares de los datos personales de pedir la rectificación, la actualización, la supresión de sus datos o el olvido, así como respecto al plazo de conservación; y (ii) que todos los nodos de la red pueden ver la información, lo cual también podría estar vulnerando la reserva y el consentimiento otorgado por el titular de los datos.

Asimismo, con las redes sociales y los buscadores –como son por ejemplo: Google, Facebook, Twitter, LinkedIn, entre otras– también sucede que *"Internet ha puesto en circulación en la globosfera millones de datos sobre todos nosotros, algunos de ellos facilitados por nosotros mismos, no siempre con la precaución de que debiéramos –dicho sea de paso–, y en otras ocasiones esas informaciones provienen de terceros que las suben a la red, con o sin nuestro consentimiento.*[490] *"*

Todas estas nuevas tecnologías se han venido desarrollando en los últimos años y no hay dudas acerca del gran impacto que han generado en corto plazo. Basta con indicar que Google se creó en el año 1998 y que tiene en el entorno de 500 millones de usuarios activos al mes. Facebook se creó en el año 2004 y se estima que tiene aproximadamente 2100 millones de usuarios activos cada mes. Twitter se creó en el

488 MELL P., GRANCE T, definition of cloud computing. Commun ACM. 2010;53(6):50. Citado en BID: "Servicios sociales para ciudadanos digitales. Oportunidades para América Latina y el Caribe", pp 26. URL: https://publications.iadb.org/es/servicios-sociales-para-ciudadanos-digitales-oportunidades-para-america-latina-y-el-caribe Consultado el 15 de setiembre de 2019.

489 Obra citada, pp. 26.

490 SANJURJO REBOLLO, BEATRIZ, obra citada, pág. 179.

2006 y se estima que tiene 320 millones de usuarios activos por mes. Instagram se lanzó en el 2010 y tiene más de 800 millones de usuarios activos por mes. Snapchat se lanzó en el 2011 y tiene más de 255 millones de usuarios[491].

Como se ha señalado, la UE trabaja para alcanzar el MUD para lo cual busca ¨*lograr que la economía, la industria y la sociedad europea aproveche plenamente la nueva era digital. Junto con las soluciones y datos electrónicos, y con los servicios digitales transfronterizos, forma parte integrante del proyecto de una Europa digital concebido por la UE.*¨[492]

Como parte de la estrategia se destaca la modernización de la protección de datos, así como la portabilidad transfronteriza de contenidos en línea. Mas para que el objetivo se pueda alcanzar es de suma importancia seguir expandiendo la economía digital y derribar los muros reglamentarios entre los diversos estados miembros de la UE[493].

En este sentido, interesa destacar que mientras los Reglamentos son actos legislativos vinculantes que se aplican de forma directa e íntegra por todos los estados miembros; las Directivas son actos legislativos que establecen objetivos y corresponde a cada estado miembro determinar la forma en que alcanza esos objetivos, lo cual les otorga mayor discrecionalidad a los países miembros.

Ante todo este nuevo contexto de nuevas tecnologías, innovaciones, necesidades y desafíos; en la UE regía la Directiva del año 1995, la cual otorgaba cierta discrecionalidad a los estados miembros en lo que respecta a la protección y disponía determinados requisitos para la transferencia internacional de DP con terceros países.

En vista de toda esta nueva realidad y tras que Edward Snowden revelara sobre los programas de vigilancia masiva llevados a cabo por diversos países, la Naciones Unidas dictó la Resolución 68/167, de 18 diciembre de 2013, y la 69/166, de 18 de diciembre de 2014 sobre el derecho a la privacidad en la era digital; reconociendo, entre otras cosas, que: la privacidad: (i) es un derecho humano que debe protegerse también en Internet, (ii) *"la vigilancia y la interceptación ilícitas o arbitrarias de las comunicaciones*, así como la recopilación ilícita o arbitraria de datos personales, al

[491] MEJIA, JUAN CARLOS, ¨Estadísticas de redes sociales 2018¨. URL: https://www.juancmejia.com/marketing-digital/estadisticas-de-redes-sociales-usuarios-de-facebook-instagram-linkedin-twitter-whatsapp-y-otros-infografia/#1_Usuarios_activos_de_Facebook Consultado el 15 de setiembre de 2019.
[492] Consejo Europeo, URL: https://www.consilium.europa.eu/es/policies/digital-single-market/
[493] Íbídem.

constituir actos de intrusión grave, violan el derecho a la privacidad y pueden interferir con el derecho a la libertad de expresión y ser contrarios a los preceptos de una sociedad *democrática, en particular cuando se llevan a cabo a gran escala"*[494]*;* (iii) la vigilancia debe ser compatible con las obligaciones internacionales en materia de derechos humanos y debe realizarse sobre la base de un marco jurídico que sea de acceso público, claro, preciso, amplio y no discriminatorio[495]; (iv) solo se permiten injerencias si no son arbitrarias ni ilegales, teniendo en cuenta lo que sea razonable para la persecución de objetivos legítimos; (v) las limitaciones deben estar establecidas por ley y no pueden vaciar su esencia; (vi) los Estados deben adoptar las medidas necesarias para hacer efectivos los derechos reconocidos a las personas; (viii) se requiere para el ejercicio de otros derechos como ser: la libertad de expresión, la no discriminación y la asociación[496].

Como se adelantó, en la Unión Europea se había aprobado en el año 1995 la Directiva 95/46/CE, que tenía como objetivo "*Proteger los derechos y las libertades de las personas en lo que respecta al tratamiento de datos personales, estableciendo los criterios fundamentales para que el tratamiento sea lícito y los principios relativos a la calidad de los datos".* Se complementaba con la Directiva 2002/58/CE, modificada por la 2009/136/CE, que se aplicaba al tratamiento de datos personales en relación con la prestación de los servicios de comunicaciones electrónicas disponibles al público en las redes públicas de telecomunicaciones. Además, con la Decisión 2000/520/CE, que hacía alusión al Artículo 25.1 de la Directiva 95/46/CE que prohibía la transferencia de Datos Personales a países que no garanticen un nivel de protección adecuado, y al artículo 25.6 de la Directiva 95/46/CE, que buscaba que terceros países garantizaran la protección adecuada o sustancialmente equivalente. Se presumía adecuada el nivel de protección para la transferencia de datos en el caso de empresas de Estados Unidos siempre que: (1) cumplieran con los "Principios de Puerto Seguro", (2) siguieran con las Directrices de aplicación (Preguntas Frecuentes), (3) publicaran sus políticas de privacidad, y (4) se sometieran a la jurisdicción de la Federal Trade Comission Act.

El "Principio de Puerto Seguro" era de decisión voluntaria, había que declararlo públicamente, así como establecer un programa autorregulado de protección de la vida

494 Naciones Unidas, El derecho a la privacidad en la era digital, Res.69/166.
495 Naciones Unidas, El derecho a la privacidad en la era digital, Res.69/166.
496 Naciones Unidas: "El derecho a la privacidad en la era digital" de 20 de junio de 2014.

privada. Se tenía que garantizar una vía de recursos independiente, asequible e inmediata, procedimientos de seguimiento, la obligación de subsanar los problemas derivados de incumplimientos y que se aplicaran sanciones. Se disponían límites, como ser: exigencias de seguridad nacional, interés público y cumplimiento de la ley, por disposición legal o reglamentaria, por excepción o dispensa establecida en la Directiva o normas de derecho interno.

El Caso ¨Maximilam Schrems vs. Irish Data Protection Comissioner¨ vino a modificar las soluciones existentes. El Sr. Schrems presentó una demanda ante la Autoridad Irlandesa de Control de Protección de Datos Personales contra Facebook, pidiendo que se prohibiera transferir sus datos personales a Estados Unidos, alegando que no se le garantizaba protección suficiente, en tanto tras las revelaciones realizadas por Snowden en el año 2013, surgía que la Agencia de Seguridad Nacional de Estados Unidos, monitorizaba de forma indiscriminada los datos personales almacenados en servidores localizados en dicho país sin respetar los límites de protección.

La Autoridad Irlandesa desestimó la demanda por el régimen de "Puerto Seguro", por lo que el Sr. Schrems procedió a presentarlo ante el Tribunal Supremo Irlandés quien lo derivó como cuestión prejudicial al Tribunal de Justicia de la Unión Europea (TJUE) y le pidió que se expida sobre si es válida o no la transferencia de datos a entidades adheridas a los Principios de Puerto Seguro.

El TJUE realizó la Comunicación 846 señalando, entre otras cosas: que varios programas de vigilancia que comprendían la recogida y el tratamiento de información a gran escala de DP podían afectar el nivel de protección de los DP de los ciudadanos de la UE transferidos a Estados Unidos, en tanto se podrían estar utilizando para fines diversos a los que se recogieron y se transfirieron.

Asimismo, el TJUE realizó la Comunicación 847 señalando, entre otras cosas que las empresas del sector de Internet no cumplían con los principios de Puerto Seguro y que tienen centenares de clientes en UE. Se teme que por el programa de recogida de información a gran escala, autoridades estadounidenses tengan acceso a DP más allá de lo necesario y proporcional para la protección de la seguridad nacional; y se reconoce que no está prevista la opción para los ciudadanos de UE de acceder, rectificar, suprimir, ni obtener reparación en lo que respecta a la recogida y tratamiento de los DP.

Analizada la temática, el TJUE constata que autoridades estadounidense podían acceder a los datos personales transferidos y tratarlos de forma incompatible con las finalidades de esa transferencia, que van más allá de lo estrictamente necesario y proporcional, y que las personas afectadas no disponen de vías judiciales ni administrativas para acceder a los datos y obtener en su caso su rectificación o supresión.

Ante dicha situación, el TJUE dicta sentencia el 6 de octubre de 2015 y declara[497] que las autoridades de control de un estado miembro de la UE pueden atender solicitudes respecto a la protección de DP que sean transferidos a terceros países, cuando se alegue que no se le garantiza una protección adecuada, e invalida la Decisión 2000/520.

En vista de estas variadas situaciones, y si bien la Directiva 95/46/CE trataba de armonizar la protección de los datos personales y garantizar la libre circulación; como surge de los Considerandos de la RGPD –entre otras cosas-:

(i) Se reconoce que el tratamiento de los datos debe concebirse para servir a la humanidad, que no es un derecho absoluto sino que debe considerarse en relación con su función en la sociedad, debiendo mantener el equilibrio con otros derechos fundamentales, con arreglo al principio de proporcionalidad.

(ii) Se destacan los retos que devienen con la rápida evolución tecnológica y con la globalización, por la magnitud de recogida de datos, así como por el gran intercambio que se realiza.

(iii) Se enfatiza el hecho de que la tecnología ha transformado la economía y la vida social, y que las personas difunden mundialmente gran volumen de su información personal.

(iv) Se subraya que esta nueva realidad requiere de un marco más sólido para la adecuada protección, esencial para otorgar confianza que permita el desarrollo de la economía digital.

(v) Se quiere que las personas tengan el control de sus DP, al tiempo que se refuerce la seguridad jurídica para las personas físicas, para los operadores económicos y para las autoridades públicas.

[497] http://curia.europa.eu/juris/document/document.jsf?docid=169195&doclang=ES Consultado el 15 de Agosto de 2019.

(vi) Se identifican los riesgos importantes para la protección de los DP en línea.

(vii) Se entiende necesario garantizar un nivel uniforme y elevado de protección, eliminando obstáculos a la circulación dentro de la UE, que otorgue seguridad jurídica y transparencia, para lo cual es esencial garantizar un tratamiento equivalente, coherente y homogéneo en todos los Estados miembros.[498]

En consecuencia el Parlamento y el Consejo Europeo aprobó el Reglamento UE 2016/679 de 27 de abril de 2016, el cual -en línea con lo establecido en el artículo 8, apartado 1, de la Carta de los Derechos Fundamentales de la Unión Europea, y el artículo 16, apartado 1, del Tratado de Funcionamiento de la Unión Europea (TFUE)- *"reconoce que toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan".* Aplicable desde el 25 de mayo de 2018[499].

Establece las normas relativas a la protección de las personas físicas en lo referente al tratamiento de sus datos personales y las normas relativas a la libre circulación de los datos (Artículo 1º del RGPD). No se aplica a la protección de DP de personas fallecidas[500], ni regula el tratamiento de DP relativos a personas jurídicas[501].

Se entiende por ¨datos personales¨ a *¨toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona¨;* y por ¨tratamiento¨ a *¨cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción¨.*[502].

[498] Considerandos (10) y (13) del Reglamento (UE) 2016/679 (RGPD).
[499] Artículo 99 del RGPD.
[500] Considerando (27) del RGPD.
[501] Considerando (14) del RGPD.
[502] *Artículo 4 del RGPD.*

La protección se aplica a la información relativa a personas físicas identificadas o identificables. Para determinar si una persona física es identificable, deben tenerse en cuenta todos los medios que razonablemente se puedan utilizar para ello (por ejemplo: los costes, el tiempo y la tecnología disponible). La protección no alcanza a la información anónima, que no guarda relación con una persona física identificada o identificable, ni a los datos convertidos en anónimos de forma que el interesado no sea identificable.

El RGPD aplica al tratamiento de DP contenidos o destinados a ser incluidos en ficheros, ya sea que vayan a ser tratados de forma automatizada o no (Artículo 2 del RGPD), previendo expresamente los casos en que no se aplica[503].

Se entiende por ¨fichero¨: *¨todo conjunto estructurado de datos personales, accesibles con arreglo a criterios determinados, ya sea centralizado, descentralizado o repartido de forma funcional o geográfica¨*[504].

Se considera ¨responsable del tratamiento ¨ a ¨*la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento*[505]¨ y al ¨encargado del tratamiento¨ a ¨*la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento*¨[506].

---

[503] *Artículo 2 del RGPD: ¨2. El presente Reglamento no se aplica al tratamiento de datos personales:*
a) en el ejercicio de una actividad no comprendida en el ámbito de aplicación del Derecho de la Unión; b) por parte de los Estados miembros cuando lleven a cabo actividades comprendidas en el ámbito de aplicación del capítulo 2 del título V del TUE;
c) efectuado por una persona física en el ejercicio de actividades exclusivamente personales o domésticas;
d) por parte de las autoridades competentes con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales, o de ejecución de sanciones penales, incluida la de protección frente a amenazas a la seguridad pública y su prevención.
3. El Reglamento (CE) nº 45/2001 es de aplicación al tratamiento de datos de carácter personal por parte de las instituciones, órganos y organismos de la Unión. El Reglamento (CE) nº 45/2001 y otros actos jurídicos de la Unión aplicable a dicho tratamiento de datos de carácter personal se adaptarán a los principios y normas del presente Reglamento de conformidad con su artículo 98.
4. El presente Reglamento se entenderá sin perjuicio de la aplicación de la Directiva 2000/31/CE, en particular sus normas relativas a la responsabilidad de los prestadores de servicios intermediarios establecidos en sus artículos 12 a 15.¨
[504] Artículo 4, numeral 6) del RGPD.
[505] Artículo 4, numeral 7) del RGPD.
[506] Artículo 4, numeral 8) del RGPD.

Entre las principales innovaciones de la norma se suelen destacar las siguientes: (i) ámbito de aplicación, extraterritorialidad de la norma; (ii) responsabilidad proactiva; (iii) se refuerza el consentimiento y la forma en que se debe comunicar a las personas sobre sus DP; (iv) nuevos derechos, se refuerza el derecho al olvido y se establece el de portabilidad de los datos; (v) privacidad desde el diseño y por defecto; (vi) notificación de las brechas de seguridad a los interesados y a las autoridades; (vii) designar a un delegado de protección de datos personales; (viii) grandes sanciones.

Se proceden a comentar.

(II.1) Ámbito de aplicación, extraterritorialidad de la norma.

Una de las grandes innovaciones del RGPD es su ámbito de aplicación territorial, lo cual es una garantía adicional para los ciudadanos, en tanto pretende adaptar los criterios que determinan qué empresas deben cumplirlo ampliándolo a la realidad del mundo de internet, lo cual permite que sea aplicable a empresas que, hasta ahora, podían estar tratando datos de personas en la UE y, sin embargo, se regían por normativas que no siempre ofrecen el mismo nivel de protección que la normativa europea. De esta manera, busca atender la nueva realidad del mundo digital y proteger los derechos fundamentales de las personas. En este sentido, el RGPD protege el DP independiente de a donde vaya.[507]

(II.2) Responsabilidad proactiva.

El artículo 5 del RGPD prevé la responsabilidad proactiva del responsable de los DP y los principios que rigen el tratamiento:

- licitud, lealtad y la transparencia;
- limitación a la finalidad explícita, legítima y determinada;
- minimización a aquellos adecuados, pertinentes y necesarios;
- exactos y actualizados;

[507] El artículo 3 del RGPD dispone que se aplica al tratamiento de DP: (1) en el contexto de actividades de un establecimiento en la UE, independientemente de que dicho tratamiento tenga lugar en la UE o no; (2) de interesados que residen en la UE por parte de un responsable o encargado no establecido en la UE, cuando las actividades estén relacionadas con: (a) oferta de bienes y servicios en la UE, independientemente de si se requiere pago o no, o (b) el control de comportamiento en la UE; (3) por parte de un responsable que no esté establecido en la UE, mas que el Derecho de los Estados miembros le sea de aplicación por el Derecho internacional público.

- conservados por el plazo necesario para los fines del tratamiento;
- aplicación de medidas técnicas u organizativas apropiadas para garantizar su integridad y confidencialidad.

Esta responsabilidad también se exige para los temas de seguridad. Al respecto en el Considerando (85) del RGPD destaca la importancia de tomar medidas adecuadas a tiempo ante violaciones de la seguridad de los DP, en tanto pueden generar muchos daños y perjuicios, materiales e inmateriales, pudiendo generar perjuicios económicos y sociales (por ejemplo: pérdidas financieras, reversión de la seudonimización, daños en la reputación, vulneración de secretos profesionales, etc).

(II.3) Se refuerza el consentimiento y la forma en que se debe comunicar a las personas sobre sus DP.

El responsable tiene que ser capaz de demostrar que el interesado consintió el tratamiento de sus DP. En caso de que lo haya otorgado en un contexto de declaración escrita, el consentimiento se tiene que distinguir claramente de los demás asuntos, de forma inteligible y de fácil acceso, utilizando lenguaje claro y sencillo.

En lo que respecta a la transparencia, a la comunicación y a las modalidades de ejercicio de los derechos del interesado, el artículo 12 del RGPD destaca las medidas oportunas que deben tomarse para informar al interesado en relación a sus DP (artículos 13 y 14 del RGPD), y en relación a la comunicación relativa al tratamiento, se subraya la forma en que la misma se debe realizar: *¨en forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo, en particular cualquier información dirigida específicamente a un niño. La información será facilitada por escrito o por otros medios, inclusive, si procede, por medios electrónicos.¨*[508]

(II.4) Nuevos derechos, se refuerza el derecho al olvido y se establece el de portabilidad de los datos.

Además de los derechos ARCO (Acceso, Rectificación, Cancelación y Oposición), se disponen nuevos derechos a los interesados como son el Derecho al Olvido y el Derecho a la Portabilidad de los Datos.

[508] Artículo 12 del RGPD.

El Derecho al Olvido ya había sido reconocido anteriormente, en particular el Tribunal de Justicia de la Unión Europea (TJUE) en el año 2014 en un caso entre la Agencia Española de Protección de Datos y la filial española de Google.

Considerando (65) del RGPD señala que los interesados tienen derecho a que se rectifiquen los DP y derecho al olvido. *¨En particular, los interesados deben tener derecho a que sus datos personales se supriman y dejen de tratarse si ya no son necesarios para los fines para los que fueron recogidos o tratados de otro modo, si los interesados han retirado su consentimiento para el tratamiento o se oponen al tratamiento de datos personales que les conciernen, o si el tratamiento de sus datos personales incumple de otro modo el presente Reglamento. Este derecho es pertinente en particular si el interesado dio su consentimiento siendo niño y no se es plenamente consciente de los riesgos que implica el tratamiento, y más tarde quiere suprimir tales datos personales, especialmente en internet. El interesado debe poder ejercer este derecho aunque ya no sea un niño. Sin embargo, la retención ulterior de los datos personales debe ser lícita cuando sea necesaria para el ejercicio de la libertad de expresión e información, para el cumplimiento de una obligación legal, para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento, por razones de interés público en el ámbito de la salud pública, con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, o para la formulación, el ejercicio o la defensa de reclamaciones.*

(66) A fin de reforzar el «derecho al olvido» en el entorno en línea, el derecho de supresión debe ampliarse de tal forma que el responsable del tratamiento que haya hecho públicos datos personales esté obligado a indicar a los responsables del tratamiento que estén tratando tales datos personales que supriman todo enlace a ellos, o las copias o réplicas de tales datos. Al proceder así, dicho responsable debe tomar medidas razonables, teniendo en cuenta la tecnología y los medios a su disposición, incluidas las medidas técnicas, para informar de la solicitud del interesado a los responsables que estén tratando los datos personales."

En definitiva, el derecho a la supresión o al olvido[509] se presenta como el derecho que tienen las personas a que se supriman sus DP cuando: (i) los datos ya no sean necesarios con los fines para los que fueron recogidos o hayan sido tratado de otro

[509] Artículo 17 del Reglamento UE 2016/679

modo, (ii) el interesado dio el consentimiento para uno o varios fines específicos, y no se base en otro fundamento jurídico, (iii) el interesado se oponga al tratamiento por motivos relacionados con su situación particular o tengan por objeto la mercadotecnia, y no prevalezcan otros motivos legítimos para el tratamiento, (iv) los DP hayan sido tratados ilícitamente;(v) los DP deban suprimirse para el cumplimiento de una obligación legal establecida en el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento; (vi) los DP se hayan obtenido en relación con la oferta de servicios de la sociedad de la información con el consentimiento de un niño, menor de 16 años, siendo lícito únicamente si el consentimiento lo dio o autorizó el titular de la patria potestad o tutea sobre el niño, y solo en la medida en que se dio la autorización.

Por otra parte, el derecho a la portabilidad de los datos[510], como informa el Grupo de Trabajo sobre Protección de Datos Personales, el derecho está estrechamente relacionado con el derecho de acceso, pero difiere del mismo en muchos aspectos.

"Permite a los interesados recibir los datos personales, que han proporcionado a un responsable del tratamiento, en un formato estructurado, de uso común y legible por máquina, así como transmitirlos a otro responsable del tratamiento. El propósito de este nuevo derecho es capacitar al interesado y darle más control sobre los datos personales que le afectan.

Puesto que permite la transmisión directa de datos personales de un responsable del tratamiento a otro, el derecho a la portabilidad de los datos es también una herramienta importante que respaldará la libre circulación de datos personales en la UE y promoverá la competencia entre los responsables del tratamiento. Facilitará el

[510] Artículo 20 del Reglamento UE 2016/679: *"Derecho a la portabilidad de los datos 1. El interesado tendrá derecho a recibir los datos personales que le incumban, que haya facilitado a un responsable del tratamiento, en un formato estructurado, de uso común y lectura mecánica, y a transmitirlos a otro responsable del tratamiento sin que lo impida el responsable al que se los hubiera facilitado, cuando: a) el tratamiento esté basado en el consentimiento con arreglo al artículo 6, apartado 1, letra a), o el artículo 9, apartado 2, letra a), o en un contrato con arreglo al artículo 6, apartado 1, letra b), y b) el tratamiento se efectúe por medios automatizados. 2. Al ejercer su derecho a la portabilidad de los datos de acuerdo con el apartado 1, el interesado tendrá derecho a que los datos personales se transmitan directamente de responsable a responsable cuando sea técnicamente posible. 3. El ejercicio del derecho mencionado en el apartado 1 del presente artículo se entenderá sin perjuicio del artículo 17. Tal derecho no se aplicará al tratamiento que sea necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento. 4. El derecho mencionado en el apartado 1 no afectará negativamente a los derechos y libertades de otros"*

poder cambiar entre diferentes proveedores de servicios y, por lo tanto, promoverá el desarrollo de nuevos servicios en el contexto de la estrategia de mercado único digital.[511]*"* (en adelante, ¨MUD¨).

Como se desprende del artículo, la portabilidad de datos permite al interesado recibir los datos personales que le incumban, que haya facilitado a un responsable del tratamiento, en un formato estructurado, de uso común y lectura mecánica, y transmitirlos a otro responsable del tratamiento sin que lo impida el responsable al que se los hubiera facilitado, cuando: (a) el interesado dio su consentimiento para el tratamiento con uno o varios fines o cuando es necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de éste de medidas precontractuales, y (b) el tratamiento se realice por medios automatizados.

(II.5) Privacidad desde el diseño y por defecto.

Se entiende necesario la adopción de medidas técnicas y organizativas que sean adecuada para proteger los DP y garantizar el cumplimiento del RGPD. Para esto se exige que el responsable del tratamiento adopte poíticas internas y aplique medidas que cumplan con la protección de los DP desde el diseño y por defecto. Dichas medidas podrían consistir en: (i) reducir al máximo el tratamiento de DP, (ii) seudonimizar lo antes posible los DP, (iii) dar transparencia a las funciones y al tratamiento de DP, (iv) permitir a los interesados supervisar el tratamiento de los DP, (v) habilitar que el responsable del tratamiento cree y mejore elementos de seguridad, (vi) alentar a los productores de productos y a los desarrolladores de servicios y aplicaciones a que tengan en cuenta el derecho a la protección de DP, (vii) asegurar que los responsables y los encargados del tratamiento están en condiciones de proteger los DP.[512]

En esta línea, el artículo 25.1 del RGPD dispone en relación al *¨diseño"* que *¨el responsable del tratamiento aplicará, tanto en el momento de determinar los medios de tratamiento como en el momento del propio tratamiento, medidas técnicas y organizativas apropiadas, como la seudonimización, concebidas para aplicar de forma efectiva los principios de protección de datos, como la minimización de datos, e*

511 https://www.agpd.es/portalwebAGPD/temas/reglamento/common/pdf/directricesportabilidad.pdf Consultado el 15 de setiembre de 2019.

512 Considerando (78) del RGPD.

integrar las garantías necesarias en el tratamiento, a fin de cumplir los requisitos del presente Reglamento y proteger los derechos de los interesados.¨

Asimismo, en relación a *¨por defecto¨*, el artículo 25.2 del RGPD, refiere a la utilización de los DP que sean necesarios para los fines específicos del tratamiento – aplicando a la cantidad de DP recogidos, a la extensión, al plazo de conservación y a su accesibilidad-, y a que sean accesibles[513] a un número determinado de personas.[514]

Para acreditar que se cumple con la protección de los DP desde el diseño y por defecto, se prevé un mecanismo de certificación en el artículo 42 del RGPD que permite acreditar el cumplimiento.

Al respecto, el artículo 42 prevé, a fin de demostrar el cumplimiento de lo dispuesto en el RGPD en las operaciones de tratamiento de los responsables y de los encargados, promover la creación de mecanismos de certificación en materia de protección de datos y de sellos o marcas de protección de datos.

Asimismo, en el apartado 2, el artículo 42 también dispone la posibilidad de establecer mecanismos de certificación, sellos o marcas de protección de datos con el objeto de demostrar la existencia de garantías adecuadas ofrecidas por los responsables o encargados no sujetos al Reglamento en el marco de transferencias de DP a terceros países u organizaciones internacionales de aplicar garantías adecuadas. *¨Dichos responsables o encargados deberán asumir compromisos vinculantes y exigibles, por vía contractual o mediante otros instrumentos jurídicos vinculantes, para aplicar dichas garantías adecuadas, incluidas las relativas a los derechos de interesados¨*[515].

Se señala que la certificación es voluntaria, que estará disponible a través de un proceso transparente y que será expedida por los organismos de certificación a que refiere el artículo 43 del RGPD o por la autoridad competente de control – de conformidad con lo establecido en el artículo 58, apartado 3, del RGPD- o por el

[513] El Diccionario de la Real Academia Española define *¨Accesible¨* como: *¨1. Que tiene acceso. 2. De fácil acceso o trato. 3. De fácil comprensión, inteligible.¨* ; y *¨Acceso¨* como *¨1. Acción de llegar o acercarse. 2. Entrada o paso. 3. Entrada al trato o comunicación con alguien¨*.

[514] Artículo 25.2 del RGPD: *¨El responsable del tratamiento aplicará las medidas técnicas y organizativas apropiadas con miras a garantizar que, por defecto, solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento. Esta obligación se aplicará a la cantidad de datos personales recogidos, a la extensión de su tratamiento, a su plazo de conservación y a su accesibilidad. Tales medidas garantizarán en particular que, por defecto, los datos personales no sean accesibles, sin la intervención de la persona, a un número indeterminado de personas físicas.¨*

[515] Apartado 2, artículo 42 del RGPD.

Comité Europeo de Protección de Datos (creado por el artículo 68 del RGPD) conforme con el artículo 63 del RGPD.

Finalmente destacar que a los efectos de contribuir a la correcta aplicación del RGPD, se promueve la elaboración de códigos de conducta (artículo 40 del RGPD), teniendo en cuenta las características específicas de los distintos sectores de tratamiento y las necesidades específicas.

(II.6) Notificación de las brechas de seguridad a los interesados y a las autoridades.

Como se señala en el Considerando (85) y en el Artículo 33 del RGPD ante violaciones de la seguridad de los DP el responsable del tratamiento debe notificar a la autoridad de control competente, sin dilación indebida y de ser posible, a más tardar a las 72 horas desde que haya tenido constancia de ella. A menos que sea improbable que dicha violación de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas.

La notificación debe contemplar como mínimo la siguiente información:

- describir la naturaleza de la violación de la seguridad;
- señalar las categorías y el número aproximado de interesados y de registros de DP;
- comunicar el nombre y los datos de contacto del delegado de protección de datos o de otro punto de contacto en el que pueda obtenerse más información;
- detallar las posibles consecuencias de la violación de la seguridad;
- referir las medidas adoptadas o propuestas por el responsable del tratamiento para remediar la violación de la seguridad de los DP, incluyendo –si corresponde- las medidas adoptadas para mitigar los posibles efectos negativos.

El responsable del tratamiento debe documentar toda violación a la seguridad de los DP, incluidos los hechos relacionados, sus efectos y las medidas correctivas adoptadas.

Asimismo, el artículo 34 del RGPD dispone que cuando sea probable que la violación de la seguridad de los DP contenga un alto riesgo para los derechos y

libertades de las personas físicas, el responsable del tratamiento lo comunicará al interesado sin dilación indebida.

La comunicación se debe realizar en un lenguaje claro y sencillo, debe explicar la naturaleza de la violación de la seguridad de los DP, así como informar del detalle antes señalado remitido en la notificación a la autoridad competente.

Sin perjuicio, se dispone que la comunicación al interesado no será necesaria si se cumple alguna de las condiciones siguientes:

a) si se tomaron medidas de protección técnicas y organizativas previas que hagan ininteligibles los datos personales para cualquier persona que no esté autorizada a acceder a ellos, como el cifrado;

b) si se tomaron medidas ulteriores que garanticen que ya no exista la probabilidad de que se concretice el alto riesgo para los derechos y libertades del interesado;

c) si supone un esfuerzo desproporcionado, en cuyo caso se optará por una comunicación pública o una medida semejante por la que se informe de manera igualmente efectiva a todos los interesados.

(II.7) Designar a un delegado de protección de datos personales.

El artículo 37.1 del RGPD prevé la designación de un delegado de protección de datos por parte del responsable y del encargado del tratamiento siempre que:

¨el tratamiento lo realice una autoridad u organismo público, excepto los tribunales que actúen en ejercicio de su función judicial;

las actividades principales del responsable o del encargado consistan en operaciones de tratamiento que, debido a su naturaleza, alcance y/o fines, requieran una observación habitual y sistemática de interesados a gran escala, o

las actividades principales del responsable o del encargado consistan en el tratamiento a gran escala de categorías especiales de datos personales con arreglo al artículo 9 y de datos relativos a condenas e infracciones penales a que se refiere el artículo 10. ¨

Asimismo, se dispone que se podrá designar un único delegado de protección de datos cuando:

- Si se trata de un grupo empresarial –entendiendo por tal un grupo constituido por una empresa que ejerce el control y sus empresas controladas[516]- siempre que sea fácilmente accesible desde los diversos establecimientos.

- Si el responsable o el encargado del tratamiento es una autoridad u organismo público, se tendrá en cuenta su estructura organizativa y tamaño.

- Si se trata de casos distintos a los dipuestos en el 37.1, mencionados, el responsable o el encargado del tratamiento o las asociaciones y otros organismos que representen a categorías de responsables o encargados, podrá actuar por cuenta de estas asociaciones y otros organismos que representen a responsables o encargados.

Para su designación habrá que atender sus cualidades profesionales, sus conocimientos especializados del Derecho, a la práctica en materia de protección de datos y a su capacidad para desempeñar las funciones que dispone el RGPD en el artículo 39.

Al respecto, en el artículo 39 del RGPD se señala que como mínimo tendrá las siguientes funciones: *¨informar y asesorar al responsable o al encargado del tratamiento y a los empleados que se ocupen del tratamiento de las obligaciones que les incumben en virtud del RGPD y de otras disposiciones de protección de datos de la Unión o de los Estados miembros;*

supervisar el cumplimiento de lo dispuesto en el RGPD, de otras disposiciones de protección de datos de la Unión o de los Estados miembros y de las políticas del responsable o del encargado del tratamiento en materia de protección de datos personales, incluida la asignación de responsabilidades, la concienciación y formación del personal que participa en las operaciones de tratamiento, y las auditorias correspondientes;

ofrecer el asesoramiento que se le solicite acerca de la evaluación de impacto relativa a la protección de datos y supervisar su aplicación de conformidad con el artículo 35 (Evaluación de impacto relativo a la protección de datos);

cooperar con la autoridad de control;

[516] Artículo 3, numeral 19, del RGPD.

actuar como punto de contacto de la autoridad de control para cuestiones relativas al tratamiento, incluida la consulta previa a que se refiere el artículo 36, y realizar consultas, en su caso, sobre cualquier otro asunto. ¨

Asimismo, se dispone que podrá formar parte de la plantilla del responsable o del encargado del tratamiento o desempeñar sus funciones en el marco de un contrato de servicios; y que el responsable o el encargado del tratamiento publicaran los datos de contacto del delegado de protección de datos y los comunicaran a la autoridad de control.

(II.8) Grandes sanciones.

Como se indica en el Considerando (148) del RGPD, a fin de fortalecer su aplicación, cualquier infracción será castigada con sanciones, incluidas multas administrativas, con carácter adicional a medidas adecuadas impuestas por la autoridad de control o en sustitución. La imposición de sanciones debe estar sujeta a garantías procesales suficientes, como ser el derecho a la tutela judicial efectiva y a un proceso con todas las garantías.

Por otra parte, el Considerando (149) del RGPD señala que los Estados miembros deben tener la posibilidad de establecer normas en materia de sanciones penales por infracciones al RGPD, como ser autorizar la privación de los beneficios obtenidos en infracción del RGPD, sin que se vulneren el principio ne bis in idem, según la interpretación del Tribunal de Justicia.

Finalmente, dispone el Considerando (150) que a fin de reforzar y armonizar las sanciones administrativas por infracción al RGPD, cada autoridad de control debe estar facultada para imponer multas administrativas.

En vista de lo expuesto, el artículo 83 del RGPD establece las condiciones generales para la imposición de multas administrativas, destacando que sean en cada caso individual efectivas, proporcionadas y disuasorias.

Asimismo, señala que ¨se impondrán a título adicional o sustitutivo de las medidas contempladas en el artículo 58, apartado 2, letras a) a h) y j).

Al decidir se debe tener en cuenta:

¨a) la naturaleza, gravedad y duración de la infracción, teniendo en cuenta la naturaleza, alcance o propósito de la operación de tratamiento de que se trate así como

el número de interesados afectados y el nivel de los daños y perjuicios que hayan sufrido;

b) la intencionalidad o negligencia en la infracción;

c) cualquier medida tomada por el responsable o encargado del tratamiento para paliar los daños y perjuicios sufridos por los interesados;

d) el grado de responsabilidad del responsable o del encargado del tratamiento, habida cuenta de las medidas técnicas u organizativas que hayan aplicado en virtud de los artículos 25 y 32;

e) toda infracción anterior cometida por el responsable o el encargado del tratamiento;

f) el grado de cooperación con la autoridad de control con el fin de poner remedio a la infracción y mitigar los posibles efectos adversos de la infracción;

g) las categorías de los datos de carácter personal afectados por la infracción;

h) la forma en que la autoridad de control tuvo conocimiento de la infracción, en particular si el responsable o el encargado notificó la infracción y, en tal caso, en qué medida;

i) cuando las medidas indicadas en el artículo 58, apartado 2, hayan sido ordenadas previamente contra el responsable o el encargado de que se trate en relación con el mismo asunto, el cumplimiento de dichas medidas;

j) la adhesión a códigos de conducta en virtud del artículo 40 o a mecanismos de certificación aprobados con arreglo al artículo 42, y

k) cualquier otro factor agravante o atenuante aplicable a las circunstancias del caso, como los beneficios financieros obtenidos o las pérdidas evitadas, directa o indirectamente, a través de la infracción.[517]

Dependiendo el tipo de infracción, el artículo 83 del RGPD dispone que se sancionarán:

Con multas administrativas de 10 000 000 EUR como máximo o, tratándose de una empresa, de una cuantía equivalente al 2 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía:

[517] Artículo 83, apartado 2, del RGPD.

a) las obligaciones del responsable y del encargado a tenor de los artículos 8, 11, 25 a 39, 42 y 43;

b) las obligaciones de los organismos de certificación a tenor de los artículos 42 y 43;

c) las obligaciones de la autoridad de control a tenor del artículo 41, apartado 4.

con multas administrativas de 20 000 000 EUR como máximo o, tratándose de una empresa, de una cuantía equivalente al 4 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía:

a) los principios básicos para el tratamiento, incluidas las condiciones para el consentimiento a tenor de los artículos 5, 6, 7 y 9;

b) los derechos de los interesados a tenor de los artículos 12 a 22;

c) las transferencias de datos personales a un destinatario en un tercer país o una organización internacional a tenor de los artículos 44 a 49;

d) toda obligación en virtud del Derecho de los Estados miembros que se adopte con arreglo al capítulo IX;

e) el incumplimiento de una resolución o de una limitación temporal o definitiva del tratamiento o la suspensión de los flujos de datos por parte de la autoridad de control con arreglo al artículo 58, apartado 2, o el no facilitar acceso en incumplimiento del artículo 58, apartado 1.

f) El incumplimiento de las resoluciones de la autoridad de control a tenor del artículo 58, apartado 2

En definitiva, La actualización era necesaria, basta con pensar todos los cambios vinculados con la tecnología y las telecomunicaciones que ocurrieron en estos últimos 20 años.

Lo que se busca, entre otras cosas, es asegurar que la obtención, el tratamiento y el mantenimiento de los datos personales se realice para la finalidad indicada, para el objetivo u objetivos declarados y autorizados, para los cuales se recogieron, que se juntan solo los necesarios para ese fin, que se conservan en forma segura, por el tiempo preciso y que la persona dueña de los datos mantiene el control sobre los mismos.

En lo que respecta al cumplimiento, lo primero es clasificar la información en datos personales, datos sensibles y datos no personales.

Como ya se señaló, se entiende por datos personales: *¨toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona*[518]¨.

Vale destacar que se incorpora como información personal aquella relativa a los datos de localización y los datos de identificación en línea, lo cual incluye las direcciones IP y las cookies.

Los datos sensibles[519], merecen especial protección, por su naturaleza, en tanto podrían implicar riesgos para los derechos y las libertades fundamentales. Se incluyen dentro de esta categoría aquellos que releven origen racial o étnico, opiniones políticas, creencias, afiliaciones sindicales, procesamiento de datos genéticos, datos relativos a la salud, así como los vinculados a la vida u orientación sexual de una persona física.

La innovación en este punto es que incluyen los relacionados a los datos genéticos (*relativos a las características genéticas heredadas o adquiridas de una persona física que proporcionen una información única sobre la fisiología o la salud de esa persona, obtenidos en particular del análisis de una muestra biológica de tal persona*[520]) y los biométricos (*obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos*[521]).

Los datos no personales son, por defectos, aquellos que no quedan dentro de ninguna de estas categorías. Hay que tener cuidado con aquellos datos desestructurados, como son documentos, reportes, entre otros, en tanto puede que contengan datos personales y no se advierta.

---

[518] Artículo 4 del RGPD.
[519] (51) del RGPD.
[520] Artículo 4 del GDPR.
[521] Idem.

Lo segundo que tenemos que hacer es evaluar e identificar los riesgos para la privacidad que pueden existir en los sistemas informáticos que se van a utilizar, así como en las operaciones de procesamiento de tratamiento que se van a realizar.

Al realizar este análisis van a surgir diversas cuestiones, como por ejemplo: (1) ¿qué tipo de información personal se va a recolectar?, (2) ¿cómo se va a procesar la información personal? (por ejemplo: se va a usar, a almacenar, a transmitir), (3) ¿la vamos a compartir?, ¿por qué, cómo y a dónde?, (4) ¿cómo estamos protegiendo la información de un uso inadecuado?

Por otra parte, es esencial crear un Plan de Respuesta a Incidentes. En el mismo nos debemos plantear lo siguiente: (1) cómo vamos a responder rápidamente a un quiebre de seguridad, (2) cómo vamos a considerar el alcance y el tipo de evento, (3) cómo vamos a parar el evento si está en proceso, (4) cómo vamos a mitigar los efectos, (5) cómo vamos a responder e informar a la autoridad de control de datos, si corresponde hacerlo, (6) cómo vamos a acceder y comunicar al propietario de los datos, (7) cómo nos vamos a asegurar de que ese evento no se repita.

Se suele indicar la importancia de establecer estándares que garanticen la seguridad de los datos, se suelen utilizar los ISO 28.001 y 28.002.

En caso de que utilicemos servicios de cloud computing, es importante tener presente que estaríamos haciendo transferencia de datos por lo que es primordial tener en cuenta el sitio en el que estarán alojados los datos.

Al respecto, interesa destacar a la fecha han sido declarados de nivel de protección adecuada los siguientes países o territorios: (I) *Suiza. Decisión 2000/518/CE de la Comisión, de 26 de julio de 2000;* (II) *Canadá. Decisión 2002/2/CE de la Comisión, de 20 de diciembre de 2001, respecto de las entidades sujetas al ámbito de aplicación de la ley canadiense de protección de datos;* (III) *Argentina. Decisión 2003/490/CE de la Comisión, de 3 de junio de 2003;* (IV) *Guernsey. Decisión 2003/821/CE de la Comisión, de 21 de noviembre de 2003;* (V) *Isla de Man. Decisión 2004/411/CE de la Comisión, de 28 de abril de 2004;* (VI) *Jersey. Decisión 2008/393/CE de la Comisión, de 8 de mayo 2008* ; (VI) I*slas Feroe. Decisión 2010/146/UE de la Comisión, de 5 de marzo de 2010; (VII) Andorra. Decisión 2010/625/UE de la Comisión, de 19 de octubre de 2010;* (VIII) *Israel. Decisión 2011/61/UE de la Comisión, de 31 de enero de 2011;* (IX) *Uruguay. Decisión 2012/484/UE, de la Comisión de 21 de agosto de*

2012; (X) *Nueva Zelanda. Decisión 2013/65/UE de la Comisión, de 19 de diciembre de 2012;* (XI) *Estados Unidos. Aplicable a las entidades certificadas en el marco del Escudo de Privacidad UE-EE.UU. Decisión (UE) 2016/1250 de la Comisión, de 12 de julio de 2016.*

(II.9) La protección de los DP en España y el Impacto del RGPD

Si bien, como se adelantó, España cuenta con regulación específica en la materia desde larga data, aprobó la Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales, Nº 3/2018, con el objeto de adaptarse al RGPD y de garantizar los derechos digitales de la ciudadanía.

Pero la norma va mucho más allá y partiendo de la base de que Internet se ha convertido en una realidad omnipresente, identificando los riesgos y oportunidades que ofrece, impulsa una política para hacer efectivo el pleno derecho de los derechos fundamentales en Internet.

La Ley cuenta con noventa y siete artículos. Como surge del preámbulo:

El Título I, establece las disposiciones generales y regula el objeto de la ley orgánica que es: (1) lograr la adaptación del ordenamiento jurídico español al RGPD, y establecer que el derecho fundamental de las personas físicas a la protección de datos personales se ejercerá con arreglo a lo establecido en el RGPD y en esta ley orgánica, y (2) garantizar los derechos digitales de los ciudadanos, al amparo del artículo 18.4 de la Constitución.

Destaca la regulación de los datos de las personas fallecidas. Los excluye del ámbito de aplicación y permite que las personas vinculadas al fallecido -por razones familiares o de hecho o sus herederos- puedan solicitar el acceso, así como su rectificación o supresión, en su caso con sujeción a las instrucciones del fallecido. También excluye los tratamientos que se rijan por normativas sobre protección de materias clasificadas.

El título II, establece los principios de protección de datos. Dispone: la exactitud de los datos[522], el deber de confidencialidad[523], el consentimiento del afectado para el

[522] Artículo 4 de la LOPDGDD.

[523] Artículo 5 de la LOPDGDD. Alcanza a los responsables y encargados del tratamiento de datos, así como toda persona que intervenga en cualquier fase. Esta obligación es complementaria del secreto profesional, y se mantiene aunque hubiese finalizado la relación con el encargado o el responsable del tratamiento.

tratamiento de los DP[524], la edad de 14 años para que el consentimiento de los menores sea válido para el tratamiento de los DP, un régimen especial cuando el tratamiento sea por obligación legal, interés público o ejercicio de poderes público, establece categorías especiales de datos y una disposición específica para los DP de naturaleza penal.

El Título III, trata sobre los derechos de las personas, toma el principio de transparencia y recoge información por capas, facilitando información básica e indicando una dirección electrónica u otro medio que permita acceder de forma sencilla e inmediata a la restante información[525].

El capítulo II del este título prevé el ejercicio de los derechos reconocidos en los artículos 15 a 22 del RGPD, señalando que podrán ejercerse directamente o por medio de representante legal o voluntario.

Entre los derechos se destacan: el acceso, la rectificación, la supresión, la portabilidad y la oposición.

El Título IV regula tratamientos específicos, no siendo exhaustivo de los tratamientos lícitos.

El Título V refiere al Responsable y al encargado del tratamiento. El capítulo I trata sobre las medidas de responsabilidad activa, señala que "*Los responsables y encargados, teniendo en cuenta los elementos enumerados en los artículos 24 y 25 del*

[524] Artículo 6 de la LOPDGDD. El consentimiento es toda manifestación de voluntad libre, específica, informada e inequívoca por la que acepta el tratamiento de los DP que le conciernen. Interesa destacar que no puede supeditarse la ejecución de un contrato a que el afectado consienta el tratamiento de sus DP para finalidades que no tengan relación con el contrato. Además cabe destacar que el artículo 7 de la LOPDGDD prevé un régimen especial para el consentimiento de los menores de edad, disponiendo que el tratamiento de sus DP solo puede fundarse en el consentimiento del menor si es mayor de 14 años.

[525] El artículo 11.2 establece la información básica que debe contener: *"a) La identidad del responsable del tratamiento y de su representante, en su caso. b) La finalidad del tratamiento. c) La posibilidad de ejercer los derechos establecidos en los artículos 15 a 22 del Reglamento (UE) 2016/679." Además, "si los datos obtenidos del afectado fueran a ser tratados para la elaboración de perfiles, la información básica comprenderá asimismo esta circunstancia. En este caso, el afectado deberá ser informado de su derecho a oponerse a la adopción de decisiones individuales automatizadas que produzcan efectos jurídicos sobre él o le afecten significativamente de modo similar, cuando concurra este derecho de acuerdo con lo previsto en el artículo 22 del Reglamento (UE) 2016/679." "3. Cuando los datos personales no hubieran sido obtenidos del afectado, el responsable podrá dar cumplimiento al deber de información establecido en el artículo 14 del Reglamento (UE) 2016/679 facilitando a aquel la información básica señalada en el apartado anterior, indicándole una dirección electrónica u otro medio que permita acceder de forma sencilla e inmediata a la restante información. En estos supuestos, la información básica incluirá también: a) Las categorías de datos objeto de tratamiento. b) Las fuentes de las que procedieran los datos."*

Reglamento (UE) 2016/679, determinarán las medidas técnicas y organizativas apropiadas que deben aplicar a fin de garantizar y acreditar que el tratamiento es conforme con el citado reglamento, con la presente ley orgánica, sus normas de desarrollo y la legislación sectorial aplicable." El capítulo II refiere al acceso por parte del encargado del tratamiento. El capítulo III profundiza sobre el delegado de PD. Finalmente, el capítulo IV trata sobre los códigos de conducta y certificación, señalando que serán vinculantes para quienes se adhieran a los mismos y que podrán tener mecanismos de resolución de conflictos extrajudicialmente.

El Título VI es sobre la transferencia internacional de DP.

El Título VII sobre las autoridades de PD: la Agencia Española de Protección de Datos[526], que se regirá por el RGPD, por la LOPDGDD y sus disposiciones de desarrollo, complementariamente en cuanto sea compatible con el Régimen Jurídico del Sector Púbico. Por otra parte, están las autoridades autonómicas de PD, que podrán ejercer las funciones y potestades establecidas en los artículos 57 y 58 del RGPD en determinados supuestos[527]. Y finalmente, se prevé la cooperación institucional y la coordinación.

---

[526] *"Artículo 44. Disposiciones generales.*
1. La Agencia Española de Protección de Datos es una autoridad administrativa independiente de ámbito estatal, de las previstas en la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, con personalidad jurídica y plena capacidad pública y privada, que actúa con plena independencia de los poderes públicos en el ejercicio de sus funciones.
Su denominación oficial, de conformidad con lo establecido en el artículo 109.3 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, será «Agencia Española de Protección de Datos, Autoridad Administrativa Independiente».
Se relaciona con el Gobierno a través del Ministerio de Justicia.
2. La Agencia Española de Protección de Datos tendrá la condición de representante común de las autoridades de protección de datos del Reino de España en el Comité Europeo de Protección de Datos.
3. La Agencia Española de Protección de Datos y el Consejo General del Poder Judicial colaborarán en aras del adecuado ejercicio de las respectivas competencias que la Ley Orgánica 6/1985, de 1 julio, del Poder Judicial, les atribuye en materia de protección de datos personales en el ámbito de la Administración de Justicia."

[527] *"Artículo 57. Autoridades autonómicas de protección de datos.*
1. Las autoridades autonómicas de protección de datos personales podrán ejercer, las funciones y potestades establecidas en los artículos 57 y 58 del Reglamento (UE) 2016/679, de acuerdo con la normativa autonómica, cuando se refieran a:
a) Tratamientos de los que sean responsables las entidades integrantes del sector público de la correspondiente Comunidad Autónoma o de las Entidades Locales incluidas en su ámbito territorial o quienes presten servicios a través de cualquier forma de gestión directa o indirecta.

El Título VIII prevé los procedimientos en caso de posible vulneración de la normativa de PD, en aquellos supuestos en que un afectado denuncie que no se ha atendido su solicitud de ejercer los derechos establecidos en los artículos 15 a 22 del RGPD. El procedimiento será ante la Agencia Española de Protección de Datos Personales y se prevé que el Gobierno regulará los procedimientos. Sin perjuicio, se prevé que el plazo para resolver el procedimiento será de seis meses desde que se notifique al reclamante la admisión del trámite, teniendo el silencio efecto positivo.

El Título IX establece el régimen sancionador, disponiendo que están sometidos al régimen previsto en el RGPD: los responsables y encargados de los tratamientos, los representantes de los responsables o encargados de los tratamientos no establecidos en territorio de la UE, las entidades de certificación y las entidades acreditadas de supervisión de los códigos de conducta. No siendo aplicable para el delegado de PD.

Finalmente, el Título X prevé las garantías de los derechos digitales señalando en el artículo 79, los derechos en la Era Digital: *"Los derechos y libertades consagrados en la Constitución y en los Tratados y Convenios Internacionales en que España sea parte son plenamente aplicables en Internet. Los prestadores de servicios de la sociedad de la información y los proveedores de servicios de Internet contribuirán a garantizar su aplicación."*

En este sentido, procede a reconocer y garantizar diversos derechos digitales, conforme al artículo 18.4 de la Constitución.

Se destaca:

- El derecho a la neutralidad de Internet: previendo el deber de los proveedores de servicios de ofrecer una oferta transparente, sin discriminación, ya sea por motivos técnicos o económicos[528].

---

b) Tratamientos llevados a cabo por personas físicas o jurídicas para el ejercicio de las funciones públicas en materias que sean competencia de la correspondiente Administración Autonómica o Local.
c) Tratamientos que se encuentren expresamente previstos, en su caso, en los respectivos Estatutos de Autonomía.
2. Las autoridades autonómicas de protección de datos podrán dictar, en relación con los tratamientos sometidos a su competencia, circulares con el alcance y los efectos establecidos para la Agencia Española de Protección de Datos en el artículo 55 de esta ley orgánica."

[528] Artículo 80 de la Ley 3/2018.

- El Derecho al acceso universal a Internet: independientemente de su condición social, económica o geográfica. Debiendo ser universal, asequible, de calidad y no discriminatoria. Buscando superar la brecha de género, generacional, atendiendo los entornos rurales y condiciones de igualdad[529]. En esta línea, en el artículo 97 de la LOPDGDD se prevé que el Gobierno, en colaboración con las comunidades autónomas, elaborarán un plan de Acceso a Internet con el fin de: (a) superar la brecha digital y garantizar el acceso a internet de colectivos vulnerables o con necesidades especiales, (b) impulsar la existencia de espacios de conexión de acceso público, y (c) fomentar medidas educativas que promuevan la formación en competencias y habilidades digitales básicas a personas y colectivos en riesgos de exclusión digital y la capacidad de todas las personas para que puedan hacer un uso autónomo y responsable de Internet y de las nuevas tecnologías.

- El Derecho a la Seguridad digital: tanto en lo que respecta a las comunicaciones que transmitan como las que reciban, debiendo los proveedores informar a los usuarios[530].

- Derecho a la educación digital: se garantizará la inserción de todos en la sociedad digital y el aprendizaje para poder hacer un uso seguro de los medios digitales, conforme a la dignidad humana, a los valores constitucionales, los derechos fundamentales, la intimidad personal y la protección de datos personales[531]. Asimismo, se prevé que los profesores recibirán las competencias digitales y la formación necesaria para poder enseñar y garantizar la inserción de todos. También deberán adaptarse los planes de estudio de los títulos universitarios y las pruebas de acceso de las administraciones públicas.

Se protegerá especialmente a los menores en Internet: se procurará un uso equilibrado y responsable de los dispositivos digitales, a fin de garantizar el adecuado desarrollo de la personalidad, preservar la dignidad y los derechos fundamentales[532]. En esa línea, se prevé que la utilización o difusión de imágenes o información personal de menores en las redes sociales puede implicar una intromisión ilegítima en los derechos fundamentales del menor y

[529] Artículo 81 de la Ley 3/2018.
[530] Artículo 82 de la Ley 3/2018.
[531] Artículo 83 de la Ley 3/2018.
[532] Artículo 84 de la Ley 3/2018.

podrá determinar la intervención del Ministerio Fiscal. Asimismo, se prevé la aprobación de un Plan de Actuación para promover acciones de formación, difusión y concienciación necesarias para lograr que los menores de edad hagan un uso equilibrado y responsable de los dispositivos digitales y de las redes sociales y de los servicios de la sociedad de la información[533]. Por otra parte, se prevé la protección de los datos de los menores en Internet, debiendo garantizarse el interés superior del menor y sus derechos fundamentales[534].

- Derecho de rectificación en Internet, previendo el derecho a la libertad de expresión, así como el deber de los responsables de sociales y servicios equivalente de adoptar protocolos para posibilitar el derecho de rectificación[535].

- Derecho de actualización, se dispone el derecho a solicitar a los medios de comunicación digitales la inclusión de un aviso de actualización suficientemente visible junto a las noticias que le conciernan cuando la información de la noticia original ya no refleje la situación actual[536].

- Derechos digitales relacionados con el ámbito laboral:

- Derecho a la intimidad y al uso de dispositivos digitales: *"Los empleadores deberán establecer criterios de utilización de los dispositivos digitales respetando en todo caso los estándares mínimos de protección de su intimidad de acuerdo con los usos sociales y los derechos reconocidos constitucional y legalmente. En su elaboración deberán participar los representantes de los trabajadores.*

El acceso por el empleador al contenido de dispositivos digitales respecto de los que haya admitido su uso con fines privados requerirá que se especifiquen de modo preciso los usos autorizados y se establezcan garantías para preservar la intimidad de los trabajadores, tales como, en su caso, la determinación de los períodos en que los dispositivos podrán utilizarse para fines privados.[537]"

[533] Artículo 97.2 de la Ley 3/2018.
[534] Artículo 92 de la Ley 3/2018.
[535] Artículo 85 de la Ley 3/2018.
[536] Artículo 86 de la Ley Nº 3/2018.
[537] Artículo 87 de la Ley Nº 3/2018.

- Derecho a la desconexión digital: *"a fin de garantizar, fuera del tiempo de trabajo legal o convencionalmente establecido, el respeto de su tiempo de descanso, permisos y vacaciones, así como de su intimidad personal y familiar*[538]*".* La forma de implementarlo dependerá de la naturaleza y del objeto de la relación laboral.

- Derecho a la intimidad frente a la videovigilancia: *"los empleadores habrán de informar con carácter previo, y de forma expresa, clara y concisa, a los trabajadores o los empleados públicos y, en su caso, a sus representantes, acerca de esta medida."* No podrán establecerse en los lugares destinados al descanso o esparcimiento de los trabajadores o los empleados públicos, como por ejemplo: vestuarios, comedores, aseos y lugares análogos[539].

- Derecho a la intimidad ante la geolocalización: *"Con carácter previo, los empleadores habrán de informar de forma expresa, clara e inequívoca a los trabajadores o los empleados públicos y, en su caso, a sus representantes, acerca de la existencia y características de estos dispositivos. Igualmente deberán informarles acerca del posible ejercicio de los derechos de acceso, rectificación, limitación del tratamiento y supresión.*[540] *"*

En la negociación colectiva: se podrá establecer en los convenios colectivos garantías adicionales relacionadas a los derechos y libertades vinculados con el tratamiento de los DP de los trabajadores[541].

- Derecho al Olvido: se prevé específicamente para las búsquedas en Internet[542] y en los servicios de redes sociales y servicios equivalentes[543]. Vale

[538] Artículo 88 de la Ley Nº 3/2018.
[539] Artículo 89 de la Ley Nº 3/2018.
[540] Artículo 90 de la Ley Nº 3/2018.
[541] Artículo 91 de la Ley Nº 3/2018.
[542] *"Artículo 93 de la Ley Nº 3/2018. Derecho al olvido en búsquedas de Internet.*
1. Toda persona tiene derecho a que los motores de búsqueda en Internet eliminen de las listas de resultados que se obtuvieran tras una búsqueda efectuada a partir de su nombre los enlaces publicados que contuvieran información relativa a esa persona cuando fuesen inadecuados, inexactos, no pertinentes, no actualizados o excesivos o hubieren devenido como tales por el transcurso del tiempo, teniendo en cuenta los fines para los que se recogieron o trataron, el tiempo transcurrido y la naturaleza e interés público de la información.
Del mismo modo deberá procederse cuando las circunstancias personales que en su caso invocase el afectado evidenciasen la prevalencia de sus derechos sobre el mantenimiento de los enlaces por el servicio de búsqueda en Internet.

destacar que ante todos los cambios y desafíos que el desarrollo de Internet y de las tecnologías conlleva, el "derecho al olvido" se ha configurado como una importante herramienta para proteger la privacidad de las personas. Si bien se regula expresamente en el RGPD, ya había sido introducido en la Unión Europea tras el caso Google España vs. AEPD y María Costeja González (Caso C-131/12, Sentencia del Tribunal de Justicia del 13 de mayo de 2014), que estableció, entre otras, que: "*la actividad de un motor de búsqueda, que consiste en hallar información publicada o puesta en Internet por terceros, indexarla de manera automática, almacenarla temporalmente y, por último, ponerla a disposición de los internautas según un orden de preferencia determinado, debe calificarse de «tratamiento de datos personales»"* y que los motores de búsqueda *"están obligados a eliminar de la lista de resultados obtenida tras una búsqueda efectuada a partir del nombre de una persona vínculos a páginas web, publicadas por terceros y que contienen información relativa a esta persona, también en el supuesto de que este nombre o esta información no se borren previa o simultáneamente de estas páginas web, y, en su caso, aunque la publicación en dichas páginas sea en sí misma lícita."*

Este derecho subsistirá aun cuando fuera lícita la conservación de la información publicada en el sitio web al que se dirigiera el enlace y no se procediese por la misma a su borrado previo o simultáneo.

2. El ejercicio del derecho al que se refiere este artículo no impedirá el acceso a la información publicada en el sitio web a través de la utilización de otros criterios de búsqueda distintos del nombre de quien ejerciera el derecho."

[543] "*Artículo 94. Derecho al olvido en servicios de redes sociales y servicios equivalentes.*

1. Toda persona tiene derecho a que sean suprimidos, a su simple solicitud, los datos personales que hubiese facilitado para su publicación por servicios de redes sociales y servicios de la sociedad de la información equivalentes.

2. Toda persona tiene derecho a que sean suprimidos los datos personales que le conciernan y que hubiesen sido facilitados por terceros para su publicación por los servicios de redes sociales y servicios de la sociedad de la información equivalentes cuando fuesen inadecuados, inexactos, no pertinentes, no actualizados o excesivos o hubieren devenido como tales por el transcurso del tiempo, teniendo en cuenta los fines para los que se recogieron o trataron, el tiempo transcurrido y la naturaleza e interés público de la información.

Del mismo modo deberá procederse a la supresión de dichos datos cuando las circunstancias personales que en su caso invocase el afectado evidenciasen la prevalencia de sus derechos sobre el mantenimiento de los datos por el servicio.

Se exceptúan de lo dispuesto en este apartado los datos que hubiesen sido facilitados por personas físicas en el ejercicio de actividades personales o domésticas.

3. En caso de que el derecho se ejercitase por un afectado respecto de datos que hubiesen sido facilitados al servicio, por él o por terceros, durante su minoría de edad, el prestador deberá proceder sin dilación a su supresión por su simple solicitud, sin necesidad de que concurran las circunstancias mencionadas en el apartado 2."

- Derecho a la portabilidad en servicios de redes y servicios equivalente: se prevé el *"derecho a recibir y transmitir los contenidos que hubieran facilitado a los prestadores de dichos servicios, así como a que los prestadores los transmitan directamente a otro prestador designado por el usuario, siempre que sea técnicamente posible*[544]*"*

- Derecho al testamento digital: las personas legitimadas, conforme a la norma, podrán decidir si mantener o eliminar los perfiles personales de personas fallecidas en redes sociales o servicios equivalentes, a menos que el fallecido hubiera decidido acerca de esta circunstancia, en cuyo caso se estará a sus instrucciones[545].

Como surge de lo expuesto, España lleva una gran trayectoria trabajando sobre la temática, revisten especial interés los derechos consagrados como de la era digital. No solo se transpone el RGPD, sino que se va más allá, procurando atender la nueva realidad, procurando salvaguardar los derechos fundamentales de las personas.

(II.10)La protección de los DP en Uruguay y el Impacto del RGPD

Los datos personales son cualquier tipo de información *¨referida a personas físicas o jurídicas determinadas o determinables¨* (artículo 4, literal d, de la Ley Nº 18.331).

Su protección es un derecho inherente a la persona humana, comprendido en el artículo 72 de la Constitución de la República (artículo 1 de la Ley Nº 18.331), aplica por extensión a las personas jurídicas en lo que corresponda (artículo 2 de la Ley Nº 18.331), y alcanza a aquellos datos que estén registrados en cualquier soporte que haga posible su tratamiento (artículo 3 de la Ley Nº 18.331).

Se exceptúan expresamente aquellas bases de datos: (a) mantenidas para fines exclusivamente personales o domésticos; (b) que tengan por objeto la seguridad pública, la defensa y seguridad del Estado, así como sus actividades en materia penal, investigación y represión del delito; y (c) creadas y reguladas por leyes especiales (artículo 3 de la Ley Nº 18.331).

Los principios generales que rigen la protección de los datos personales son los siguientes:

[544] Artículo 95 de la Ley Nº 3/2018.
[545] Artículo 96 de la Ley Nº 3/2018.

legalidad[546]*:* las bases de datos deben: inscribirse, atender el ordenamiento jurídico nacional y no pueden tener finalidades que contradigan los derechos humanos, el ordenamiento jurídico nacional o la moral pública.

veracidad[547]*:* los datos que se recogen en las bases de datos tienen que ser veraces, adecuados, ecuánimes -los justos y necesarios para el fin- y no excesivos. Además tienen que ser exactos, actualizarse y eliminarse cuando hayan caducado. Su recolección no puede hacerse por medios desleales, fraudulentos, abusivos o extorsivos.

finalidad[548]*:* los datos solo pueden ser utilizados para el destino para el que fueron recogidos y deben ser eliminados una vez que hayan dejado de ser necesarios o pertinentes para dicho fin. La reglamentación determina los casos y procedimientos en que se pueden conservarse aun cuando haya vencido la necesidad, por ejemplo: valores históricos, estadísticos o científicos[549].

previo consentimiento informado[550]*:* el tratamiento de DP requiere que previamente el titular de esos datos haya dado su consentimiento de forma libre, expresa e informada, lo cual debe documentarse. Asimismo, es esencial para que el consentimiento sea válido –y no se considere nulo- que se le informe al titular de los DP la finalidad para la que se destinarán y el tipo de actividad desarrollada por el responsable de la base o del tratamiento[551].

La regla es el previo consentimiento informado, las excepciones están prevista en la norma, debiéndose interpretar de forma estricta. Los casos en que no se requiere consentimiento previo son cuando: ¨a) *Los datos provengan de fuentes públicas de información, tales como registros o publicaciones en medios masivos de comunicación. B) Se recaben para el ejercicio de funciones propias de los poderes del Estado o en virtud de una obligación legal. C) Se trate de listados cuyos datos se limiten en el caso de personas físicas a nombres y apellidos, documento de identidad, nacionalidad, domicilio y fecha de nacimiento. En el caso de personas jurídicas, razón social, nombre de fantasía, registro único de contribuyentes, domicilio, teléfono e identidad de las personas a cargo de la misma. D) Deriven de una relación contractual, científica o*

[546] Artículo 6 de la Ley Nº 18.331.
[547] Artículo 7 de la Ley Nº 18.331.
[548] Artículo 8 de la Ley Nº 18.331.
[549] Artículo 38 del Decreto Nº 414/2009, Reglamentación de la Ley Nº 18.331.
[550] Artículo 9 de la Ley Nº 18.331, modificada por el artículo 152 y 156 de la Ley Nº 18.719 y por el artículo 84 de la ley Nº 19.255.
[551] Artículo 5 del Decreto Nº 414/2009, Reglamentación de la Ley Nº 18.331.

profesional del titular de los datos, y sean necesarios para su desarrollo o cumplimiento. E) Se realice por personas físicas para su uso exclusivo personal, individual o doméstico.¨[552]

seguridad de los datos[553]*:* el responsable de la base de datos tiene que garantizar la seguridad y la confidencialidad de los DP, disponiendo de condiciones técnicas de integridad y seguridad. Se tiene que evitar la adulteración, la pérdida, la consulta o el tratamiento no autorizado, así como detectar posibles riesgos. Asimismo, se tienen que almacenar de manera tal que permitan que sus titulares puedan ejercer sus derechos sobre los mismos.

En caso de que se conozca la ocurrencia de vulneraciones de seguridad en cualquier fase del tratamiento, que pudieran vulnerar significativamente los derechos de los titulares, se deberá informar de dicho extremo.

En esta línea, el artículo 38 de la Ley Nº 19.670 prevé que ¨*Cuando el responsable o encargado de una base de datos o de tratamiento, tome conocimiento de la ocurrencia de la vulneración de seguridad, deberá informar inmediatamente y pormenorizadamente de ello y de las medidas que adopte, a los titulares de los datos y a la Unidad Reguladora y de Control de Datos Personales, la que coordinará el curso de acción que corresponda, con el Centro Nacional de Respuesta a Incidentes de Seguridad Informática del Uruguay (CERTuy)*

La reglamentación determinará el contenido de la información correspondiente a la vulneración de seguridad¨.

En vista de lo expuesto, el responsable o encargado de una base de datos tiene las siguientes obligaciones:

Tomar medidas proactivas para garantizar la seguridad y la confidencialidad, debiendo evitar la adulteración, la perdida, el tratamiento no autorizado, etc..

Informar en caso de que ocurra una vulneración en cualquier fase del tratamiento, en cuanto se tenga conocimiento del quebrantamiento:

el Decreto Nº 414/2009 prevé el que se debe informar en caso de que se pudiera vulnerar significativamente los derechos de los titulares, mas la Ley Nº 19.670 no

[552] ibídem.
[553] Artículo 10 de la Ley Nº 18.331.

distingue el tipo ni la gravedad de la vulneración. Habrá que atender si la reglamentación de la Ley Nº 19.670 dispone algo respecto.

se debe informar inmediatamente y de forma pormenorizada lo ocurrido y las medidas adoptadas, a:

los titulares de los datos,

a la URCDP la que coordinará con CERTuy[554].

reserva[555]*:* el tratamiento de la base de datos tiene que hacerse de forma reservada, está prohibido su difusión a terceros, y exclusivamente para el giro o actividad autorizado.

Se establece el secreto profesional respecto de aquellas personas que por su trabajo tengan relación, acceso o intervengan en cualquier fase del tratamiento de una base de datos, cuando hayan sigo recogidas de fuentes no accesibles al público. Esta obligación subsiste aún luego de finalizada la relación con el responsable de la base de datos.

Se exceptúan los casos en que haya orden de la Justicia competente o si mediare consentimiento del titular.

Además el artículo 40 de la Ley Nº 19.670 dispone que aquellas entidades (públicas, privadas, estatales o no estatales) que traten datos sensibles como negocio principal y las que traten grandes volúmenes de datos deben designar un delegado de protección de datos.

El delegado debe ser idóneo para sus funciones y actuar con autonomía técnica. Entre las funciones se destacan: (A) asesorar en la formación, diseño y aplicación de políticas, (B) supervisar el cumplimiento, (C) proponer medidas para adecuarse a los estándares internacionales, y (D) ser un nexo entre su entidad y la URCDP.

(v) responsabilidad[556]*:* la persona física o jurídica, pública o privada, propietaria de la base de datos o que decida sobre la finalidad, contenido y uso del

[554] El Decreto 451/009 regula el funcionamiento y organización del CERTuy. El Decreto 452/009 regula la adopción de una política de seguridad de la información para organismos de la Administración Pública. Decreto 92/014 referente a la ciberseguridad, con el objetivo de mejorar la seguridad de la información y las infraestructuras tecnológicas que le dan soporte.
[555] Artículo 11 de la Ley Nº 18.331.
[556] Artículo 12 de la Ley Nº 18.331, sustituido recientemente por el artículo 38 de la Ley de Rendición de Cuentas y Balance de Ejecución Presupuestal correspondiente al ejercicio 2017,

tratamiento, está obligado a responder por la violación de las disposición de la Ley de Protección de Datos Personales.

El artículo 39 de la Ley Nº 19.670 dispone que en ejercicio de una responsabilidad proactiva, deberá adoptar las medidas técnicas y organizativas apropiadas. Entre ellas señala: (i) privacidad desde el diseño, (ii) privacidad por defecto, (iii) evaluación de impacto a la protección de datos, entre otras, a fin de garantizar un tratamiento adecuado de los datos personales y demostrar su efectiva implementación.

La reglamentación determinará las medidas que correspondan según los tipos de datos, tratamientos y responsables, así como la oportunidad para su revisión y actualización.

Frente a la recolección de DP, sus titulares tienen derecho a saber previamente[557]: (i) cuál es la finalidad del tratamiento; (ii) quiénes son los posibles destinatarios; (iii) que existe la base de datos, de qué trata la misma, así como la identidad y el domicilio de su responsable; (iv) si las respuestas al cuestionario que se le proponga son obligatorias o facultativas; (v) las consecuencias de proporcionar los datos y de la negativa a hacerlo; (vi) sobre la posibilidad de ejercer los derechos de acceso, rectificación y supresión de los datos.

Asimismo, tienen derecho a: (i) impugnar valoraciones personales[558]; (ii) consentir o no la comunicación de sus datos, debiéndosele informar sobre la finalidad de la comunicación e identificar al destinatario o los elementos que permitan hacerlo[559]; (iii) revocar el consentimiento otorgado para la comunicación[560]; (iv) la actualización[561]; (v) la inclusión[562]; (vi) la supresión[563]; (vii) la comunicación o la cesión de datos[564]; (viii) entablar acción de protección de datos personales o habeas data.

---

aún sin número: *¨El responsable de la base de datos o tratamiento y el encargado, en su caso, serán responsables de la violación de las disposiciones de la presente ley.*
En ejercicio de una responsabilidad proactiva, deberán adoptar las medidas técnicas y organizativas apropiadas: privacidad desde el diseño, privacidad por defecto, evaluación de impacto a la protección de datos, entre otras a fin de garantizar un tratamiento adecuado de los datos personales y demostrar su efectiva implementación.
La reglamentación determinará las medidas que correspondan según los tipos de datos tratamiento y responsables, así como la oportunidad para su revisión y actuación.¨

[557] Artículo 13 de la Ley Nº 18.331.
[558] Artículo 16 de la Ley Nº 18.331.
[559] Artículo 17 de la Ley Nº 18.331.
[560] Artículo 17 de la Ley Nº 18.331.
[561] Artículo 11 del Decreto Nº 414/2009.
[562] Artículo 12 del Decreto Nº 414/2009.

Además de los DP, hay datos que tienen una protección especial, como son los datos sensibles[565], los datos relativos a la salud[566], a las telecomunicaciones[567], a bases de datos con fines publicitarios[568], a la actividad comercial o crediticia[569].

También debe tener en cuenta que la Ley de Acceso a la Información Pública Nº 18.381, prevé que es pública *¨toda información que emane o esté en posesión de cualquier organismo público, sea o no estatal, salvo las excepciones o secretos establecidos por ley, así como las informaciones reservadas o confidenciales.¨*[570].

Las excepciones a la información pública deben ser interpretadas de forma estricta[571]. Comprenden: (i) las definidas como secretas por ley, por ejemplo: el secreto profesional, el estadístico, el bancario; (ii) las de carácter reservado, por ejemplo: aquellas que comprometen la seguridad pública o la defensa nacional[572]; y (iii) las de carácter confidencial[573], por ejemplo: los DP que requieren previo consentimiento informado.

Como surge de lo expuesto, nuestro país reconoce el derecho a la protección de datos personales como inherente a la personalidad humana, estando comprendido en el artículo 72 de la Constitución de la República. Desde el año 2008, cuando se aprobó la Ley de Protección de Datos Personales – reglamentada por el Decreto Nº414/2009- y la Ley de Acceso a la Información Pública, nuestro país cuenta con legislación específica en la materia[574], habiendo sido reconocido como un país que otorga protección adecuada en lo que respecta al tratamiento automatizado de los DP por Decisión 2012/484/UE del 21 de agosto de 2012.

En dicha Decisión se sostiene:

---

[563] Artículo 13 del Decreto Nº 414/2009.
[564] Artículo 14 del Decreto Nº 414/2009.
[565] Artículo 18 de la Ley Nº 18.331.
[566] Artículo 19 de la Ley Nº 18.331.
[567] Artículo 20 de la Ley Nº 18.331.
[568] Artículo 21 de la Ley Nº 18.331, con las modificaciones introducidas por el artículo 152 de la Ley Nº 18.719.
[569] Artículo 22 de la Ley Nº 18.331.
[570] Artículo 2 de la Ley Nº 18.381.
[571] Artículo 8 de la Ley Nº 18.381.
[572] Artículo 9 de la Ley Nº 18.381.
[573] Artículo 10 de la Ley Nº 18.381.
[574] Sin perjuicio desde el año 2004 contaba con la Ley Nº 17.838 sobre Protección de Datos Personales para ser utilizados en Informes Comerciales y Acción de Habeas Data, la cual fue derogada por el artículo 48 de la Ley Nº 18.331.

- Que la Constitución de la República no reconoce expresamente el derecho a la vida privada y a la protección de DP, en tanto el catálogo de derechos fundamentales no es una lista cerrada conforme lo dispuesto en el artículo 72 de la Constitución.

- Que la Constitución de la República en su artículo 332 prevé que sus preceptos que reconocen derechos a los individuos, así como los que atribuyen facultades e imponen deberes a las autoridades públicas, no dejarán de aplicarse por falta de reglamentación específica, sino que será suplida recurriendo a los fundamentos de leyes análogas, a los principios generales de derecho y a las doctrinas generalmente admitidas.

- Que la Ley Nº 18.331 de Protección de Datos Personales se basa en gran medida en la Directiva 95/46/CE.

- Que la Ley Nº 18.331 es complementada por el Decreto Nº 414/2009 de 31 de agosto de 2009.

- Que la República Oriental del Uruguay es parte de la Convención Americana de Derechos Humanos (Pacto San José de Costa Rica), cuyo artículo 11 reconoce el derecho a la vida privada, y su artículo 30 prevé que restricciones al goce y ejercicio de los derechos y libertades reconocidas solo pueden establecerse por leyes dictadas por razones de interés general y por el fin específico.

Se concluye que Uruguay debe considerarse como un país que ofrece un nivel de protección adecuado de los datos personales transferidos desde la UE, conforme a lo dispuesto en la Directiva 95/46/CE.

Como se señaló, la Directiva 95/46/CE fue derogada por el RGPD. Al respecto vale destacar que frente a las nuevas disposiciones del RGPD, Uruguay aprobó la Ley Nº 19.670 estableciendo disposiciones sobre la materia en los artículos 37, 38, 39 y 40.

Como surge del capítulo anterior, el RGPD es de gran impacto a nivel global por el carácter extraterritorial de la norma, por todas las obligaciones que contiene y por las grandes sanciones que dispone.

Si bien Uruguay por la Decisión 2012/484/UE del 21 de agosto de 2012 se considera que es un país adecuado en lo que respecta al tratamiento automatizado de los

DP, como indica la URCDP en el informe *¨Impacto en Uruguay del nuevo Reglamento de la Unión Europea sobre protección de datos personales¨*[575], la Comisión tiene la potestad de revisar que el sistema del país no miembro, al momento no se ha realizado revisión formal respectos de los países declarados adecuados.

Como surge del artículo 45 del RGPD, la Comisión tras evaluar la adecuación del nivel de protección, establecerá un mecanismo de revisión periódica, al menos cada cuatro años, que tenga en cuenta los acontecimientos relevantes en el tercer país o en la organización internacional.

Si tras dicha revisión, se entiende que un tercer país ya no garantiza un nivel de protección adecuado, la Comisión derogará, modificará o suspenderá, en la medida que sea necesario y sin efecto retroactivo, la decisión de adecuación.

Las decisiones adoptadas por la Comisión en virtud del artículo 25, apartado 6, de la Directiva 95/46/CE –como es la Decisión 2012/484/UE que dispone la adecuación de Uruguay- permanecen en vigor hasta que sean modificadas, sustituidas o derogadas por una decisión de la Comisión.

Por otra parte, en lo que respecta al ámbito de aplicación territorial, como surge del artículo 3, apartado 2 del RGPD, aplica al tratamiento de DP de interesados que residan en la UE por parte de un responsable o encargado no establecido en la UE, cuando las actividades de tratamiento estén relacionadas con: a) la oferta de bienes o servicios a dichos interesados en la UE independientemente de si a estos se les requiere su pago, o b) el control de su comportamiento, en la medida en que este tenga lugar en la UE.

Teniendo en cuenta lo expuesto, en caso que desde Uruguay se ofrezcan bienes o servicios a personas que residan en la UE o en caso de que controlen su comportamiento, en la medida en que el mismo tenga lugar en la UE; se deberá cumplir con las disposiciones del RGPD.

Vale destacar que recientemente se aprobó la Ley Nº 19.670: Ley de Rendición de Cuentas y Balance de Ejecución Presupuestal correspondiente al ejercicio 2017, estableciendo disposiciones en los artículo 36 a 40 en línea con el RGPD.

[575]Unidad Reguladora de Protección de Datos Personales, URL: https://datospersonales.gub.uy/wps/wcm/connect/urcdp/c999a065-4daa-4d1b-8a68-369139d60145/Informe_Pérez_Asinari_Mar%C3%ADa_Verónica_2016+%281%29.pdf?MOD=AJPERES&CONVERT_TO=url&CACHEID=c999a065-4daa-4d1b-8a68-369139d60145

El artículo 37 de la Ley Nº 19.670, en línea con lo establecido en el artículo 3 del RGPD, dispone que el tratamiento de DP estará sometido a la Ley Nº 18.331, cuando se realice por un responsable o encargado de tratamiento que esté establecido en el territorio nacional. En caso de que no esté establecido en territorio nacional, la ley le aplica en los siguientes casos:

- si el tratamiento está relacionado con ofrecer bienes o servicios a personas que estén en el país o con el análisis de su comportamiento;
- si lo disponen normas de derecho internacional público o un contrato;
- si en el tratamiento se utilizan medios situados en el país, salvo que sea con fines de tránsito, aunque el responsable del tratamiento deberá designar un representante con domicilio en el país ante la URCDP.

El artículo 38 de la Ley Nº 19.670, en línea con lo establecido en los artículos 33 y 34 del RGPD, señala que *¨Cuando el responsable o encargado de una base de datos o de tratamiento, tome conocimiento de la ocurrencia de la vulneración de seguridad, deberá informar inmediatamente y pormenorizadamente de ello y de las medidas que adopte, a los titulares de los datos y a la Unidad Reguladora y de Control de Datos Personales, la que coordinará el curso de acción que corresponda, con el Centro Nacional de Respuesta a Incidentes de Seguridad Informática del Uruguay (CERTuy)¨*

La reglamentación determinará el contenido de la información.

Como ya se adelantó, el artículo 39 de la Ley Nº 19.670 modifica el principio de responsabilidad establecido en el artículo 12 de la Ley Nº 18.331, sustituyendo el artículo y estableciendo la responsabilidad del responsable y del encargado del tratamiento, quienes deberán ejercer una responsabilidad proactiva, adoptando medidas técnicas y organizativas apropiadas para garantizar un tratamiento adecuado a los DP demostrar su efectiva implementación. A modo de ejemplo enuncia: privacidad desde el diseño y por defecto, evaluar el impacto a la protección de datos. Dispone que la reglamentación deberá determinar las medidas que correspondan adoptar según los tipos de datos, tratamiento y responsables, así como la revisión y la actualización a realizar.

Finalmente el artículo 40 de la Ley Nº 19.670, en línea con lo establecido en los artículos 37 y 39 del RGPD, establece que *¨Las entidades públicas, estatales o no estatales, las privadas total o parcialmente de propiedad estatal, así como las entidades privadas que traten datos sensibles como negocio principal y las que realicen el*

tratamiento de grandes volúmenes de datos deberán designar un delegado de protección de datos.

Sus funciones principales serán:

A)Asesorar en la formulación, diseño y aplicación de políticas de protección de datos personales.

B)Supervisar el cumplimiento de la normativa sobre dicha protección en su entidad.

C)Proponer todas las medidas que entienda pertinente para adecuarse a la normativa y a los estándares internacionales en materia de protección de datos personales.

D)Actuar como nexo entre su entidad y la Unidad Reguladora y de Control de Datos Personales.

El delegado deberá poseer las condiciones necesarias para el correcto desempeño de sus funciones y actuará con autonomía técnica.¨

La ley aún no ha sido reglamentada, por lo que habrá que estar atentos a lo que en la misma se establezca. Sin perjuicio, se establecen disposiciones que son de directa aplicación.

En Uruguay el Derecho al Olvido no tiene una regulación específica, mas como surge del Dictamen Nº 17/2016 de la Unidad Reguladora y de Control de Datos Personales: (i) la publicación de datos personales en Internet constituye una hipótesis de comunicación de datos –artículo 17 de la Ley Nº 18.331–, (ii) el derecho al olvido puede considerarse una proyección de otros derechos, como ser el de supresión –artículo 15 de la Ley Nº 18.331 y artículo 13 del Decreto Nº 414/2009–, (iii) "*ante la existencia de errores, falsedades o exclusiones en alguna de las informaciones vinculadas a la persona relacionada en las publicaciones, el titular del dato podrá ejercer su derecho de supresión, en principio ante el editor de las páginas web, quien deberá dar una respuesta en el plazo de 5 días hábiles, conforme prevé la norma precitada. En caso de no obtener respuesta, el titular del dato podrá accionar de habeas data ante el Poder Judicial."*

Es interesante tener presente que en ciertas ocasiones el derecho al olvido puede colidir con otros derechos fundamentales como ser el de la libertad de expresión y el de acceso a la información, lo cual requerirá una adecuada ponderación.

En definitiva, los datos personales son parte de la dignidad y de la privacidad de las personas. Sin duda el tratamiento de los datos a través de las nuevas tecnologías permite generar grandes beneficios para la sociedad, mas entiendo esencial, entre otras cosas, que los mismos: (i) se utilicen de forma ética, protegiendo los derechos fundamentales de las personas, como son: no discriminación, privacidad y libertad de expresión; (ii) se protejan desde el diseño y de forma proactiva del acceso no autorizado, así como de otras posibles vulneraciones; (iii) se utilicen para los fines declarados y recabados; (iv) se informe claramente a los titulares y se recoja su consentimiento libre, expreso e inequívoco; (v) se traten de forma anónima, para que no se pueda determinar el titular, y (vi) se respete la información confidencial, reservada o secreta.

(II.11) Consideraciones

Internet y las nuevas tecnologías, han facilitado la creación de nuevos servicios y aplicaciones digitales, que han generado un ecosistema digital que borra fronteras, refleja que vivimos en una comunidad internacional, ofrece más acceso, empodera a las personas y genera múltiples oportunidades.

Sin duda estamos ante una economía de los datos, donde la información y la intimidad de las personas está en jaque, siendo esencial tomar medidas innovadoras para poder atender debidamente la privacidad de las personas, al tiempo que no afecten la innovación y el desarrollo.

España con la Ley Nº 3/2018 no solo ha transpuesto el RGPD en la regulación nacional, sino que además ha ido más allá, reconociendo expresamente los nuevos derechos que derivan de la era digital.

Uruguay con los artículos 72 y 332 de la Constitución, tiene la posibilidad de considerar que dichos derechos tienen un respaldo y protección constitucional, en tanto pueden considerarse como derechos inherentes a la personalidad humana, no siendo necesaria su consagración expresa para que sean reconocidos.

Sin perjuicio, considero que el reconocimiento expreso, como se hizo en España, es una buena práctica en tanto facilita la universalización y protección de los mismos.

Varios países están trabajando en este desafío. En este sentido, se destacan principalmente dos normas por su impacto y por lo innovadoras de sus soluciones. Una, como ya mencionamos y desarrollamos, es el RGPD o GDPR (por sus siglas en inglés), y la otra es la Ley de California de Protección de la Privacidad de los Consumidores, conocida como CCPA (por sus siglas en inglés). A continuación se procede a desarrollar sobre las principales diferencias y similitudes entre estas dos importantes regulaciones.

(II.12) Principales diferencias y similitudes entre GDPR y CCPA (en inglés)[576]

Which are the main similarities and differences between the General Data Privacy Regulation (GDPR) and the California Consumer Privacy Act (CCPA)?

Even though the core of GDPR and CCPA (hereinafter, "both regulations") is to protect people's privacy, they have some similarities and differences that are important to consider to comply appropriately.

In the digital era, we continuously generate and share data. There is no doubt about the benefits that the use of data has, but if we misuse it, consciously or not, we can affect people's privacy.

In this sense, new and innovative regulations have been developed looking for ways to use the data correctly to protect people's privacy, empowering and allowing them to control their data.

There are different regulations, but there are two that may have a more significant impact globally. One is the European Union (hereinafter, "EU") Regulation 2016/679, named General Data Privacy Regulation (hereinafter, "GDPR"), and the other is the California Consumer Privacy Act (hereinafter, "CCPA").

---

[576] Fuentes consultadas el 13 de mayo de 2020:
Regulation (EU) 2016/679, General Data Protection Regulation.
The California Consumer Privacy Act 2018.
https://pages.iapp.org/rs/138-EZM-042/images/Top%205%20Operational%20Impacts%20CCPA-FINAL.pdf?mkt_tok=eyJpIjoiTVRjek0yRm1PRFE0TldSaCIsInQiOiJLcFdsbVRXMDJBQ3JYcj
RFRllQOEhHa3JjNjAwVFFpbFlnZmJKWlwvelphOWt4Qm9uZnpkNWE4dVF3bmFTd0tjNmJKbk9HenJ6bEo3T0hSRm0zY3NKek9SOXptM09vQ09xb3Y0ZWI2MFwvYVc4ZitwU2lCcXVMdG1MWHc4RWJwdjlHIn0%3D
https://fpf.org/wp-content/uploads/2018/11/GDPR_CCPA_Comparison-Guide.pdf
https://www.bakerlaw.com/webfiles/Privacy/2018/Articles/CCPA-GDPR-Chart.pdf

Both are innovative, look to protect people's privacy, and recognize new rights. Nonetheless, they have some differences that are important to contemplate to comply appropriately.

In this line, I will make a general description of the GDPR and CPPA, and then I will comment on the main similarities and differences that they have. Both are extensive, complex, and innovative regulations; hence for this memorandum, I will consider only the main aspects.

(II.I12.A.) *General Data Privacy Regulation of the European Union (GDPR)*

In the EU, according to Article 8 of the Charter of Fundamental Rights, privacy is a fundamental right. The GDPR entered into force on May 25, 2018, and replaced the Data Protection Directive 95/46/EC as the leading law that protects EU citizens' personal data (hereinafter, "PD").

GDPR protects natural persons about the processing of PD and rules relating to the free movement of PD.

GDPR applies to the processing of PD wholly or partly by automated means and to the processing other than by automatic means of PD, which form part of a filing system or are intended to form part of a filing system.

PD is any information related to an identified or identifiable natural person (hereinafter, "data subject"). A natural person can be identified, directly or indirectly, by reference to an identifier such as a name, an identification number, location data, an online id or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

The processing of sensitive data that for example, reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data to uniquely identify a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation, is prohibited.

"Processing" refers to any operation or set of operations which is performed on PD, by automated means or not, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

GDPR does not apply to the processing of PD when, among other things, it is done by a natural person in the course of a merely personal or household activity, or by a competent authority for the prevention, investigation, detection or prosecution of criminal offenses or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.

GDPR applies to the processing of PD: (1) in the context of the activities of an establishment of a controller or a processor in the EU, despite where the processing takes place; or (2) of the data subject is in the EU by a controller or processor not established in the EU, where the processing activities are related to: (a) the offering of goods or services, payable or not, or (b) the monitoring of their behaviors that take place in the EU.

A controller is a natural or legal person, public authority, agency, or another body that, alone or jointly with others, determines the purposes and means of the processing PD. And the processor is the one that processes PD on behalf of the controller.

The controller to process PD properly must have accountability and demonstrate compliance with the following principles:

lawfulness, fairness, transparency, about the data subject.

Purpose limitation: PD shall be collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes. Processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes is not considered incompatible with the initial purposes.

Data minimization: PD shall be adequate, relevant, and limited to what is necessary for relation to the purposes for which it is processed.

Accuracy: PD shall be accurate and, if it is needed, kept up to date. Reasonable measures must be taken, without delay, to ensure that inaccurate PD is erased or rectified.

Storage limitation: PD shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the PD is processed.

Integrity and confidentiality: PD shall be treated in a manner that ensures proper security of the PD, using appropriate technical or organizational measures, including

protection against unauthorized or unlawful processing and accidental loss, destruction or damage.

The processing will be legitimate only if:

the data subject has given consent for the specific purposes; or if

it is necessary:

- for the performance of a contract to which the data subject is a party or to take steps at the request of the data subject before entering into a contract;
- for compliance with a legal obligation to which the controller is subject;
- to protect the vital interests of the data subject or of another natural person;
- for the performance of a task carried out in the public interest or the exercise of official authority vested in the controller;
- for the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of PD.

The controller must demonstrate that the data subject consented the processing of his or her PD appropriately and informed. Additionally, the data subject shall be able to remove the consent easily.

The child's consent to the processing of their PD is lawful if the child is at least 16 years old. The permission of children between 13 and 16 years old request authorization by the holder of parental responsibility.

The data subject has specific rights, and the controller must provide transparent information, taking appropriate measures to communicate and to allow the exercise of his or her rights.

Expressly, the GDPR set the following rights to the data subject:

Right to notice: where his or her PD is collected, and specific information such as the identity and contact details of the controller, purposes of the processing, the interest pursued, the recipients of the PD. If the PD will be transferred to a third country and the existence or absence of an adequacy decision by the Commission or an appropriate or

suitable safeguards, the period for which the PD will be stored, the rights that the data subject disposed of.

Right of access: to the PD and specific information such as for purposes of the processing, categories of PD concerned, the recipients if the PD has been or will be disclosed, the envisaged period for which the PD will be stored, the existence of her or his rights.

Right to rectification: of inaccurate PD concerning him or her.

Right to erasure (Right to be forgotten): the PD concerning him or her when among other cases: (a) it is no longer necessary for the purposes for which it was collected or otherwise processed, (b) withdraw the consent, (c) there are no overriding legitimate grounds for the processing, (d) the PD has been unlawfully processed, (e) the PD has to be erased for compliance with a legal obligation in EU, (f) the PD has been collected about an information society service.

Right to restrict the processing, to limit their processing in the future.

Right to data portability: The data subject shall have the right to receive the PD concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller

Right to object: on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her, including profiling, and when PD is processed for direct marketing purposes.

Right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly him or her. It doesn't apply if the decision is necessary: for a contract between the data subject and a data controller; or if it is authorized by the law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or if it is based on the data subject's explicit consent.

The protection has to be by design and by default considering the State of the art, the cost of implementation and the nature, scope, context, and purposes of processing as well as the risks.

In this sense, the controller shall implement appropriate technical and organizational measures to ensure a level of security, including, among other: (1) pseudonymization and encryption; (2) the ability to provide the ongoing confidentiality, integrity, availability, and resilience of processing systems and services; (3) the ability to restore the availability and access to PD promptly in the event of a physical or technical incident; (4) a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures.

In the case of a PD breach, the controller shall, not later than 72 hours after having become aware of it, notify the PD breach to the supervisory authority competent unless the breach is unlikely to result in a risk to the rights and freedoms of natural persons. Also, when the PD breach is likely to result in a high risk to the right and freedom of natural persons, the controller shall communicate the data subject without delay.

In case of infringement, the national authority shall impose administrative fines in respect to the breach, considering each fact, effectiveness, proportionality, and how dissuasive these fines can be. In some cases, penalties could be up to 20 000 000 EUR, or in the case of an undertaking, up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher.

(III.12.B.) California's Consumer Privacy Act (CCPA)

The State of California approved "The California Consumer Privacy Act of 2018" (hereinafter, "CCPA") on June 28, 2018, which went into effect last January 1, 2020.

The California Constitution grants a "right of privacy" to all people, and to ensure it, the CCPA gives to every natural person who is a California resident (hereinafter, "consumer") an effective way to control its personal information (hereinafter, "PI").

California Resident includes every individual who is in the State for other than a temporary or transitory purpose and every individual who is domiciled in the State but is outside the State for temporary or fleeting use.

PI is any "information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household". For example, it includes identifiers, commercial Information, biometric Information, Internet, or other electronic network activity information, and geolocation data.

CCPA applies to any business that collects, alone or jointly with others, consumer's PI, and meets one or more of the following thresholds:

has gross revenues over $25 million;

buys receive or sell PI of over 50,000 consumers, households, or devices annually; and

at least 50 percent of annual revenues come from selling consumers' PI.

CCPA guarantees the following rights to consumers:

Right to know what PI about him or her is being collected: whether it is sold or disclosed, and to whom. The consumer has the right to request a business that gathers PI to disclose: (i) the categories and specific pieces of PI that are being collected; (ii) the categories of sources from which PI is collected; (iii) the business or commercial purpose to collect or sell the PI; (iv) the categories of third parties with whom the business shares PI.

The business cannot collect additional types of PI or use it for other purposes without providing notice to the consumer.

Right to access his or her PI: Consumers have the right to access their PI. A business must make available to consumers two or more designated methods for submitting requests for information required to be disclosed.

A Business which receives a verifiable consumer request from a consumer to access PI, must: (i) disclose and deliver it in 45 days (which can be extended in certain circumstances), (ii) free of charge, (iii) by mail or electronically, in a readily useable format that allows to transmit it without hindrance, (iv) at any time, no more than twice in 12 months.

Right to request the deletion. A business should disclose to consumers their rights to request the removal of his or her PI. The consumer can request it at any time, and the business shall delete the PI.

However, there are the following exceptions that the business can apply to maintain the PI: (1) Complete the transaction for which it was collected, provide a good or service requested by the consumer, or otherwise perform a contract between the business and the consumer. (2) Detect security incidents, protect against malicious, deceptive, fraudulent, or illegal activity; or prosecute those responsible for that activity.

(3) Debug to identify and repair errors that impair existing intended functionality. (4) Exercise free speech, ensure the right of another consumer to exercise his or her right of free speech or exercise another right provided for by law, (5) Compliance with the California Electronic Communications Privacy Act. (6) Research in the public interest. (7) Internal uses reasonably aligned with the expectations of the consumer based on the relationship. (8) Comply with a legal obligation. (9) Other internal uses in a lawful manner.

Right to opt-out or opt-in to the sale of his PI, depending on the age.

If a business sells consumer PI, it has to inform about the consumer's right to opt-out of the sale of her or his PI at any time. In that case, the business that receives the opt-out shall be prohibited from selling it, unless the consumer subsequently provides express authorization for the sale.

If consumers are less than 16 years old, they have the right to opt-in. A business to sell the PI of consumers under 16 years old needs an affirmative authorization. If consumers are less than 13 years old, they need the written approval of a parent or guardian.

Businesses must provide a clear and noticeable link on their homepage, named "Do Not Sell My Personal Information" allowing a consumer, or a person authorized by the consumer, to opt-out. Also, along with a separate link, a business must include a description of consumers' rights according to CCPA, and its online privacy policy or policies if the business has an online privacy policy or policies.

The right to equal services and prices, even if they exercise their privacy rights.

A business cannot discriminate against consumers because of the exercising of their rights. Nonetheless, a business may offer financial incentives, including payments to consumers as compensation, for the collection, sale, or the deletion of PI. A business may also provide a different price, rate, level, or quality of goods or services to the consumer if that price or difference is directly related to the value provided to the consumer by the consumer's data.

A business that offers financial incentives shall notify consumers of the financial incentives. The consumer may give the business prior opt-in consent, which clearly describes the material terms of the financial incentive program, and which may be revoked by the consumer at any time.

A business shall not use financial incentive practices that are unfair, unreasonable, coercive, or usurious.

In case of unauthorized access and exfiltration, theft, or disclosure to the consumer PI, If it is as a result of the business' violation of the duty to implement and maintain reasonable security procedures and practices to protect the PI, the consumer may institute a civil action for any of the following: (i) To recover damages (from $100 to $750) per incident or actual damages, whichever is higher. (ii) Injunctive or declaratory relief. (iii) Any other relief the court deems proper.

A business shall be in violation if it fails to fix any alleged violation within 30 days after being notified of alleged noncompliance. The liability for violating CCPA is a civil penalty that can range from $2.500 (non-intentional) up to $7.500 (intentional), for each violation.

(II.12.C.) Analysis

Both regulations protect people's privacy, but they have some differences that are important to be aware of.

Background: GDPR replaced the previous Directive from 1998 as the main act that protects EU citizens' data. CCPA is the first act of this kind in the US, which was known as a sectoral approach applying to specific information.

Subject matter: The right to privacy is a Constitutional right, and both regulations look to ensure it.

Scope:

Subject to Protection: Both regulations protect natural people, but GDPR specifically EU citizens, and CCPA California residents.

Subject to control: GDPR regulates the controller, which can be any business or entity; CCPA applies to specific businesses that comply with particular thresholds. The Processor in the GDPR is similar to the Service Provider in the CCPA, both regulations request contracts.

Territorial: Both regulations apply in and outside their specific territorial jurisdiction.

Material: GDPR refers to PD related to an identified or identifiable natural person. In contrast, CCPA refers to PI that identifies or is capable of being associated with, directly or indirectly, with a particular consumer or household.

GDPR expressly alludes to the processing of PD by automated or non-automated means whether the PD is part of a filing system, and to the free movement. CCPA doesn't delimit it but refers to collecting, selling, processing.

Both regulations exclude processing for non-commercial activities, such as purely personal or household purposes, and do not apply to data that do not allow identifying the person such as anonymized data (GDPR) or de-identified information and aggregate consumer information (CCPA).

CCPA excludes specific categories of PD such as medical information and the publicly available one, GDPR does not exclude it from the protection.

GDPR prohibits the processing of sensitive data; CCPA does not define special categories of information as GDPR.

The consent requirements for the child is the same, providing both regulations special protection.

Both regulations define research broadly, but CCPA does not state limits to the purpose for which personal information can be used.

Responsibilities: GDPR states that the controller must have accountability and compliance with principles to process PD legally. Also, the controller must demonstrate that the data subject consented the processing of his or her PD, appropriately and informed. CCPA does not set something like that, and only sets mechanisms to opt-out and to erase the information.

Rights:

Right to notice or to inform: both regulations have similar requirements, but differences in the type of information, the time, and the methods.

The right to access or to disclosure: is similar in both regulations, but GDPR allows broader access, and is not limited to a written declaration as CCPA.

Right to rectification: GDPR provides it. CCPA does not recognize it; it only contains the right to opt-out of the sales of personal information.

Right to restriction of processing: GDPR provides it. CCPA does not recognize it; it only contains the right to opt-out of the sales of personal information.

The right to data portability: is similar in both regulations, but GDPR stipulates a specific reason.

Right to restrict and to object processing: GDPR provides it. CCPA does not recognize it; it only contains the right to opt-out of the sales of personal information.

Right not to be subject to a decision based solely on automated processing, including profiling: GDPR provides it. CCPA does not recognize it.

Right to Opt-Out for personal information sales: CCPA provides it. GDPR does not include it. However, it does offer other rights that have similar results such as withdrawal consent or opt-out of processing for marketing purposes.

Right to deletion or erasure: both regulations provide the same solution. Nonetheless, CCPA is broader, GDPR states specific conditions.

Right of non-discrimination: CCPA expressly recognizes it, in GDPR it is implicit in a different statement such as in the rights and freedom of data subjects.

Respond to requests: Both regulations provide how a business or a controller must respond, looking for verification, terms, and other special conditions.

Security: both regulations are similar, requesting reasonable and appropriate technical and organizational measures, considering the risk, and the specific circumstances.

Infringement and penalties: Both regulations state civil fines, the statements are different, but either can be a significant economic liability.

(II.12.D.) Conclusions

GDPR and CCPA are innovative and disruptive regulations that may have a high impact in a lot of organizations and businesses worldwide.

Both regulations look to protect peoples' privacy, but they have some differences that are important to consider.

Every organization that has personal data from EU citizens and/or personal information from California residents, must consider the obligations and specifications

of each regulation to comply appropriately and avoid potential infringement and penalties.

III Libertad de expresión y el acceso a la información

La sociedad de la información, empoderó a los individuos y cambió la forma en que las personas interactúan, en que se expresan, en que comparten contenido y en que acceden a la información.

Gracias a la digitalización, a la convergencia, así como a la conectividad a Internet y a las plataformas digitales, podemos expresarnos libremente, compartir información, crear contenido, llegando prácticamente a todo el mundo, en cuestión de segundos, desde cualquier sitio y a través de variedad de dispositivos.

Antes era impensable que una persona pudiera tener este alcance en sus comunicaciones. Solo lo podían llegar a tener los medios masivos de comunicación, como podía ser la televisión, la radio o el periódico; pero eran centralizados, tenían limitaciones geográficas y de autorizaciones, lo cual los hacía más fáciles de regular y de controlar.

Sin duda este empoderamiento de las personas tiene múltiples beneficios, como ser: más libertad, más información, más contenido, más acceso, más servicios y más negocios. Pero tiene su lado negativo, como puede ser la realización de conductas antisociales –por ejemplo: la difamación–, la compartición y distribución de contenidos indebidos –por ejemplo: creando y distribuyendo noticias falsas–, la vulneración de derechos de las personas –por ejemplo: la propiedad intelectual–, al tiempo que pueden ser utilizados para coordinar o realizar prácticas delictivas –por ejemplo: para reclutar jóvenes para actos ilegales–.

A través de las plataformas electrónicas y de los diversos intermediarios, las personas pueden personalizar el contenido que consumen, al tiempo que pueden generarlo y distribuir el propio y el ajeno, por todo el mundo, en cuestión de segundos. Es cierto que parte del contenido puede ser negativo para la sociedad, mas gran parte de él es muy positivo, en tanto es social o informativo, permite compartir noticias nacionales e internacionales, contenido educativo, información sobre deporte, entre otros muchos ejemplos.

El problema se plantea cuando se genera o distribuye contenido antisocial o negativo, lo cual se agrava por las particularidades de que Internet es global, se esparce rápidamente por la web, no se borra y que es difícil identificar correctamente al autor, al editor o al autor.

Este último aspecto está captando la atención y la preocupación de los reguladores y autoridades, quienes están poniendo el foco en la responsabilidad de los intermediarios o en los proveedores de acceso, generando presión y obligando a: (i) filtrar y bloquear contenidos, y (ii) develar información que puede limitar el derecho de las personas a expresarse libremente, así como a recibir información e ideas a través de cualquier medio de comunicación, lo cual es vital para la democracia moderna.

Para que los contenidos se puedan trasmitir y compartir debidamente en el mundo digital, se requiere de diversos actores que brindan servicios, conocidos generalmente como "intermediarios". Son definidos de diversas formas, mas generalmente se refiere a cualquier entidad que permita la comunicación de información[577], pudiendo ser desde los proveedores de servicios de Internet, los motores de búsqueda, los servicios de *blogs*, plataformas de comunicación en línea[578], las plataformas de comercio electrónico, servidores web, redes sociales, entre otros ejemplos[579].

En tanto tienen la posibilidad de controlar cómo, quién y qué se comparten los usuarios a través de sus plataformas, han pasado a tener un rol clave para proteger la libertad de expresión, el acceso a la información y la privacidad[580], derivando en diversas regulaciones que les atribuyen responsabilidades.

Múltiples instrumentos internacionales reconocen a la libertad de expresión como un derecho humano fundamental. Entre ellos, el artículo 19 de la DUDH[581], el artículo

577 UNESCO. Fostering Freedom Online: The role of Internet Intermediaries. Unesco Series on Internet Freedom. Internet Society (2014), pp. 19.

578 Naciones Unidas. Asamblea General. Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión, Frank La Rue. A/HRC/17/27. 16 de mayo de 2011, pp. 38.

579 Iniciativa global de la sociedad civil. Principios de Manila sobre Responsabilidad de los Intermediarios. Antecedentes. Versión 1.0. Mayo 2015, pp. 6.

580 UNESCO. Fostering Freedom Online: The role of Internet Intermediaries. Unesco Series on Internet Freedom. Internet Society (2014). pp. 23.

581 Artículo 19 de la Declaración Universal de Derechos Humanos:

"Todo individuo tiene derecho a la libertad de opinión y de expresión; este derecho incluye el de no ser molestado a causa de sus opiniones, el de investigar y recibir informaciones y opiniones, y el de difundirlas, sin limitación de fronteras, por cualquier medio de expresión."

11 de la Declaración Universal de Derechos del Hombre y del Ciudadano de 1789[582], artículo 19 del Pacto Internacional de Derechos Civiles y Políticos de 1966[583], el artículo 13 de la Convención Americana.[584] Asimismo lo ha previsto el artículo 10 de la CEDH[585] y la Primera Enmienda de la Constitución de los Estados Unidos[586].

---

582 Artículo 11 de la Declaración Universal de Derechos del Hombre y del Ciudadano de 1789: "*La libre comunicación de pensamientos y opiniones es uno de los derechos más valiosos del Hombre; por consiguiente, cualquier Ciudadano puede hablar, escribir e imprimir libremente, siempre y cuando responda del abuso de esta libertad en los casos determinados por la Ley".*

583 Artículo 19 del Pacto Internacional de Derechos Civiles y Políticos:

"1. Nadie podrá ser molestado a causa de sus opiniones.

2. Toda persona tiene derecho a la libertad de expresión; este derecho comprende la libertad de buscar, recibir y difundir informaciones e ideas de toda índole, sin consideración de fronteras, ya sea oralmente, por escrito o en forma impresa o artística, o por cualquier otro procedimiento de su elección.

3. El ejercicio del derecho previsto en el párrafo 2 de este artículo entraña deberes y responsabilidades especiales. Por consiguiente, puede estar sujeto a ciertas restricciones, que deberán, sin embargo, estar expresamente fijadas por la ley y ser necesarias para:

a. Asegurar el respeto a los derechos o a la reputación de los demás;

b. La protección de la seguridad nacional, el orden público o la salud o la moral públicas".

584 Artículo 13 de la Convención Americana:

"1. Toda persona tiene derecho a la libertad de pensamiento y de expresión. Este derecho comprende la libertad de buscar, recibir y difundir informaciones e ideas de toda índole, sin consideración de fronteras, ya sea oralmente, por escrito o en forma impresa o artística, o por cualquier otro procedimiento de su elección.

2. El ejercicio del derecho previsto en el inciso precedente no puede estar sujeto a previa censura sino a responsabilidades ulteriores, las que deben estar expresamente fijadas por la ley y ser necesarias para asegurar:

a. *el respeto a los derechos o a la reputación de los demás, o*

b. *la protección de la seguridad nacional, el orden público o la salud o la moral públicas.*

3. No se puede restringir el derecho de expresión por vías o medios indirectos, tales como el abuso de controles oficiales o particulares de papel para periódicos, de frecuencias radioeléctricas, o de enseres y aparatos usados en la difusión de información o por cualesquiera otros medios encaminados a impedir la comunicación y la circulación de ideas y opiniones.

4. Los espectáculos públicos pueden ser sometidos por la ley a censura previa con el exclusivo objeto de regular el acceso a ellos para la protección moral de la infancia y la adolescencia, sin perjuicio de lo establecido en el inciso 2.

5. Estará prohibida por la ley toda propaganda en favor de la guerra y toda apología del odio nacional, racial o religioso que constituyan incitaciones a la violencia o cualquier otra acción ilegal similar contra cualquier persona o grupo de personas, por ningún motivo, inclusive los de raza, color, religión, idioma u origen nacional".

585 Convención Europea de Derechos Humanos artículo 10:

"1. Toda persona tiene derecho a la libertad de expresión. Este derecho comprende la libertad de opinión y la libertad de recibir o de comunicar informaciones o ideas sin que pueda haber injerencia de autoridades públicas y sin consideración de fronteras. El presente artículo no impide que los Estados sometan a las empresas de radiodifusión, de cinematografía o de televisión a un régimen de autorización previa.

Interesa destacar que la diferencia principal entre lo establecido en la CEDH y la Primer Enmienda de la Constitución de Estados Unidos es relativo a las excepciones que se prevén a la libertad de expresión. Se puede afirmar que en Estados Unidos se apunta más a la libertad, al ejercicio de la autonomía individual y a la tolerancia, mientras que en la Unión Europea se busca más un balance entre la libertad de expresión y la dignidad de las personas, estableciendo más excepciones.

Como ya se adelantó, la Sección 1 de la Constitución Española, "De los derechos fundamentales y de las libertades públicas"; específicamente en su artículo 20 se reconoce y protege, entre otros derechos, el derecho a expresar y difundir libremente los pensamientos, ideas y opiniones mediante la palabra, el escrito o cualquier otro medio de reproducción, así como a comunicar o recibir libremente información veraz por cualquier medio de difusión. Asimismo indica que el "ejercicio de estos derechos no puede restringirse mediante ningún tipo de censura previa", más señala que su límite está en el respeto a los derechos fundamentales, a las libertades públicas, y especialmente en el derecho al honor, a la intimidad, a la propia imagen y a la protección de la juventud y de la infancia.

"Los derechos de comunicación son derechos fundamentales y eso se refleja en características especiales como la de que han de regularse mediante Ley Orgánica, y ello exige un quórum para su aprobación, modificación o derogación, de mayoría absoluta; de hecho, si una materia objeto de regulación mediante Ley Orgánica no fuera aprobada, modificada o derogada mediante LO, conllevaría la declaración de inconstitucional por el Tribunal Constitucional por infracción del Art. 81 CE[587] *y del Art. 28.2*[588] *de la Ley Orgánica del Tribunal Constitucional*[589].

---

2. El ejercicio de estas libertades, que entrañan deberes y responsabilidades, podrá ser sometido a ciertas formalidades, condiciones, restricciones o sanciones, previstas por la ley, que constituyan medidas necesarias, en una sociedad democrática, para la seguridad nacional, la integridad territorial o la seguridad pública, la defensa del orden y la prevención del delito, la protección de la salud o de la moral, la protección de la reputación o de los derechos ajenos, para impedir la divulgación de informaciones con denciales o para garantizar la autoridad y la imparcialidad del poder judicial".

586 Primera Enmienda de la Constitución de los Estados Unidos: *"El Congreso no hará ley alguna por la que adopte una religión como oficial del Estado o se prohiba practicarla libremente, o que coarte la libertad de palabra o de imprenta, o el derecho del pueblo para reunirse pacíficamente y para pedir al gobierno la reparación de agravios".*

587 Artículo 81:

Asimismo, nuestro texto constitucional prevé un procedimiento preferente y sumario ante los tribunales ordinarios para la defensa de los derechos de la comunicación como derechos fundamentales. El Art. 53.2 CE establece que: "cualquier ciudadano podrá recabar la tutela de las libertades y derechos reconocidos por un procedimiento basado en los principios de preferencia y sumariedad". Se establece este procedimiento preferente y sumario como una especial protección a los derechos fundamentales entendiendo esa "preferencia" frente a la lentitud del resto de casos, dotándole de una más rápida tramitación y de una duración menor, con la intención de resolver cuanto antes el litigio; y a ese requisito de preferencia se añade la "sumariedad", como una limitación de la cognición judicial o del objeto procesal a tan solo una parte del conflicto, la de los derechos fundamentales especialmente

---

1. Son leyes orgánicas las relativas al desarrollo de los derechos fundamentales y de las libertades públicas, las que aprueben los Estatutos de Autonomía y el régimen electoral general y las demás previstas en la Constitución.
2. La aprobación, modificación o derogación de las leyes orgánicas exigirá mayoría absoluta del Congreso, en una votación final sobre el conjunto del proyecto.

[588] Artículo veintiocho de la Ley Orgánica del Tribunal Constitucional.
Uno. Para apreciar la conformidad o disconformidad con la Constitución de una Ley, disposición o acto con fuerza de Ley del Estado o de las Comunidades Autónomas, el Tribunal considerará, además de los preceptos constitucionales, las Leyes que, dentro del marco constitucional, se hubieran dictado para delimitar las competencias del Estado y las diferentes Comunidades Autónomas o para regular o armonizar el ejercicio de las competencias de éstas.
Dos. Asimismo el Tribunal podrá declarar inconstitucionales por infracción del artículo ochenta y uno de la Constitución los preceptos de un Decreto-ley, Decreto legislativo, Ley que no haya sido aprobada con el carácter de orgánica o norma legislativa de una Comunidad Autónoma en el caso de que dichas disposiciones hubieran regulado materias reservadas a Ley Orgánica o impliquen modificación o derogación de una Ley aprobada con tal carácter, cualquiera que sea su contenido.

589 Capítulo IV de la Constitución: "DE LAS GARANTÍAS DE LAS LIBERTADES Y DERECHOS FUNDAMENTALES"

Artículo 53:
1. Los derechos y libertades reconocidos en el Capítulo segundo del presente Título vinculan a todos los poderes públicos. Sólo por ley, que en todo caso deberá respetar su contenido esencial, podrá regularse el ejercicio de tales derechos y libertades, que se tutelarán de acuerdo con lo previsto en el artículo 161, 1, a).
2. Cualquier ciudadano podrá recabar la tutela de las libertades y derechos reconocidos en el artículo 14 y la Sección primera del Capítulo segundo ante los Tribunales ordinarios por un procedimiento basado en los principios de preferencia y sumariedad y, en su caso, a través del recurso de amparo ante el Tribunal Constitucional. Este último recurso será aplicable a la objeción de conciencia reconocida en el artículo 30.
3. El reconocimiento, el respeto y la protección de los principios reconocidos en el Capítulo tercero informarán la legislación positiva, la práctica judicial y la actuación de los poderes públicos. Sólo podrán ser alegados ante la Jurisdicción ordinaria de acuerdo con lo que dispongan las leyes que los desarrollen.
Artículo 54: Una ley orgánica regulará la institución del Defensor del Pueblo, como alto comisionado de las Cortes Generales, designado por éstas para la defensa de los derechos comprendidos en este Título, a cuyo efecto podrá supervisar la actividad de la Administración, dando cuenta a las Cortes Generales.

protegidos, dejando la otra parte imprejuzgada; lo que, eventualmente, podrá ser objeto de enjuiciamiento en un proceso plenario ulterior. No existiendo un único proceso preferente y sumario sino que dependiendo de la materia a tratar en el litigio, nos remitiremos a las distintas jurisdicciones"[590].

En este sentido, se prevé una tutela ante los tribunales ordinarios y otra ante el Tribunal Constitucional.

Interesa destacar la Sentencia N° 159/1986 del Tribunal Constitucional en relación al artículo 20 de la Constitución Española en tanto destaca el rol de la libertad de expresión y de comunicación como principio democrático, que presupone el derecho de los ciudadanos a contar con amplia y adecuada información que les permita formar sus convicciones. Destacando que el derecho a la información además de proteger un derecho individual, es una garantía de la opinión pública, firmemente relacionada con el pluralismo político. Asimismo, destacar que subraya que cuando entra en conflicto la libertad de información con otros derechos fundamentales, las restricciones tienen que ser interpretadas de manera que su contenido no sea desnaturalizado ni incorrectamente relativizado[591].

Con el advenimiento de los nuevos servicios cada vez se presentan más espacios e instancias que facilitan la libre expresión de las personas, así como su comunicación y el alcance a la información. Al respecto, considerando la importancia que estos derechos tienen para cada individuo, así como para la sociedad, se deben considerar alcanzados

[590] SANJURJO REBOLLO B, "Manual de Internet y Redes Sociales", Dykinson, pág.47 y 48.

[591] Sentencia N° 159/1986 del Tribunal Constitucional *"El art. 20 C.E., además de consagrar el derecho a la libertad de expresión y a comunicar o recibir libremente información veraz, juega un papel esencial como garantía institucional del principio democrático que inspira nuestra Constitución, el cual presupone el derecho de los ciudadanos a contar con una amplia y adecuada información respecto a los hechos, que les permita formar sus convicciones ponderando opiniones diversas e incluso contrapuestas y participar así en la discusión relativa a los asuntos públicos. En este sentido ha manifestado reiteradamente este Tribunal (v. gr. STC 104/1986) que el derecho a la información no sólo protege un interés individual, sino que entraña «el reconocimiento y la garantía de una institución política fundamental, que es la opinión pública, indisolublemente ligada con el pluralismo político».*
7. La posición preferencial asignada al derecho fundamental reconocido en el art. 20.1 d) de la Constitución, si de una parte implica una mayor responsabilidad moral y jurídica en quien realiza la información, de otra exige una rigurosa ponderación de cualquier norma o decisión que coarte su ejercicio. Por ello, cuando la libertad de información entre en conflicto con otros derechos fundamentales e incluso con otros intereses de significativa importancia social y política, respaldados, como ocurre en el presente caso, por la legislación penal, las restricciones que de dicho conflicto puedan derivarse deben ser interpretadas de tal modo que el contenido fundamental del derecho en cuestión no resulte, dada su jerarquía institucional, desnaturalizado ni incorrectamente relativizado."

por estos derechos y por sus límites, las comunicaciones y expresiones que se realizan en el mundo digital en tanto puedan afectar los derechos de otras personas, así como perjudicar a la Sociedad.

Teniendo en cuenta lo expuesto, sin lugar a dudas los derechos de comunicaciones, de libertad de expresión y de acceso a la información por cualquier medio están teniendo cada vez mayor alcance y difusión. Son derechos esenciales para el desarrollo de todos los individuos, de la opinión pública, así como para la existencia de una sociedad libre. Mas estos derechos tienen límites: el respeto a los derechos fundamentales y a la reputación de los demás, especialmente los derechos al honor, a la intimidad, a la propia imagen y a la protección de la juventud y de la infancia, así como la protección de la seguridad nacional, el orden público o la salud o la moral públicas.

La Constitución uruguaya en el artículo 29 prevé: "*Es enteramente libre en toda materia la comunicación de pensamientos por palabras, escritos privados o publicados en la prensa, o por cualquier otra forma de divulgación, sin necesidad de previa censura; quedando responsable el autor y, en su caso, el impresor o emisor, con arreglo a la ley por los abusos que cometieren",* además se debe considerar comprendido y protegido por los artículos 7, 10 y 72 de la Constitución.

El artículo 1º de la Ley Nº 16.099, con los agregados dispuestos por la Ley Nº 18.515, dispone que: *"(Libertad de comunicación de pensamientos y libertad de información). Es enteramente libre en toda materia, la expresión y comunicación de pensamientos u opiniones y la difusión de informaciones mediante la palabra, el escrito o la imagen, por cualquier medio de comunicación, dentro de los límites consagrados por la Constitución de la República y la ley. (...)*

Constituyen principios rectores para la interpretación, aplicación e integración de las normas civiles, procesales y penales sobre expresión, opinión y difusión, relativas a comunicaciones e informaciones, las disposiciones consagradas en la Declaración Universal de Derechos Humanos, en la Convención Americana sobre Derechos Humanos y en el Pacto Internacional de Derechos Civiles y Políticos. Asimismo, se tomarán en cuenta muy especialmente los criterios recogidos en las sentencias y opiniones consultivas de la Corte Americana de Derechos Humanos y en las resoluciones e informes de la Comisión Interamericana de Derechos Humanos, siempre que ello no implique disminuir los estándares de protección establecidos en la legislación nacional o reconocidos por la jurisprudencia nacional."

Además debemos considerar el Derecho de Acceso a la Información Pública, previsto en la Ley Nº 18.381, y destacar que las disposiciones establecidas en la Ley Nº 19.307, conocida como Ley de Medios, expresamente excluyen los servicios de comunicación que utilicen como plataforma la red de protocolo de Internet.

Como ha indicado la Corte Interamericana de Derechos Humanos (CIDH)[592], *"el derecho a la libertad de pensamiento y expresión (...), contempla tanto el derecho de las personas a expresar su propio pensamiento, como el derecho a buscar, recibir y difundir informaciones e ideas de toda índole[593]. Este derecho reviste una crucial importancia para el desarrollo personal de cada individuo, para el ejercicio de su autonomía y de otros derechos fundamentales y, finalmente, para la consolidación de una sociedad democrática.[594]*

La libertad de expresión tiene dos dimensiones, (i) individual y (ii) social:

i. La individual: *"consiste en el derecho de cada persona a expresar los propios pensamientos, ideas e informaciones, y no se agota con el reconocimiento teórico del derecho a hablar o escribir, sino que comprende, inseparablemente, el derecho a utilizar cualquier medio apropiado para difundir el pensamiento y hacerlo llegar al mayor número de destinatarios"[595]*.

ii. La dimensión social *"consiste en el derecho de la sociedad a procurar y recibir cualquier información, a conocer los pensamientos, ideas e informaciones ajenos y a estar bien informada[596]. En este sentido, la Corte ha establecido que la libertad de*

592 Corte Interamericana de Derechos Humanos, Informe Nº 112/2012, Caso 12.828.

593 CIDH, Informe Nº 82/10, Caso 12.524, Fondo, Jorge Fontevecchia y Héctor d'Amico, Argentina, 13 de julio de 2010, párr. 86. Disponible en: http://www.cidh.oas.org/demandas/12.524Esp.pdf.

594 CIDH, Informe Nº. 82/10, Caso 12.524, Fondo, Jorge Fontevecchia y Héctor d'Amico, Argentina, 13 de julio de 2010, párr. 85. Cita realizada por CIDH, Informe Nº 112/2012, Caso 12.828.

595 Cfr. CIDH, La Colegiación Obligatoria de Periodistas (arts. 13 y 29 Convención Americana sobre Derechos Humanos). Opinión Consultiva OC-5/85 del 13 de noviembre de 1985. Serie A Nº. 5, párr. 31, disponible en: http://www.corteidh.or.cr/docs/opiniones/seriea_05_esp.pdf. Cita realizada por CIDH, Informe Nº 112/2012, Caso 12.828.

596 Corte I.D.H., Caso Kimel Vs. Argentina. Fondo, Reparaciones y Costas. Sentencia de 2 de mayo de 2008 Serie C Nº. 177, párr. 53; Corte I.D.H., Caso Claude Reyes y otros. Sentencia de 19 de septiembre de 2006. Serie C Nº. 151, párr. 75; Corte I.D.H., Caso López Álvarez Vs. Honduras. Sentencia de 1o de febrero de 2006. Serie C Nº. 141, párr. 163; CIDH. Alegatos ante

expresión es un medio para el intercambio de ideas e informaciones entre las personas; comprende su derecho a comunicar a otros sus puntos de vista, pero implica también el derecho de todos a conocer opiniones, relatos y noticias de toda índole libremente.[597]*"*

Finalmente destaca: *"El derecho a la libertad de expresión constituye además un elemento fundamental sobre el cual se basa la existencia de las sociedades democráticas, debido a su indispensable relación estructural con la democracia*[598]*. El objetivo mismo del artículo 13 de la Convención Americana es el de fortalecer el funcionamiento de sistemas democráticos pluralistas y deliberativos mediante la protección y el fomento de la libre circulación de información, ideas y expresiones de toda índole"*[599].

"*La libertad de expresión es una piedra angular en la existencia misma de una sociedad democrática. Es indispensable para la formación de la opinión pública. Es también conditio sine qua non para que los partidos políticos, los sindicatos, las sociedades científicas y culturales, y en general, quienes deseen influir sobre la*

---

la Corte Interamericana en el caso Herrera Ulloa Vs. Costa Rica. Transcritos en: Corte I.D.H., Caso Herrera Ulloa Vs. Costa Rica. Sentencia de 2 de julio de 2004. Serie C Nº. 107, párr. 101.1 a); Corte I.D.H., Caso Herrera Ulloa. Sentencia del 2 de julio de 2004, Serie C Nº. 107, párr. 108; Corte I.D.H., Caso Ivcher Bronstein Vs. Perú. Sentencia de 6 de febrero de 2001. Serie C Nº. 74, párr. 146; Corte I.D.H., Caso Ricardo Canese Vs. Paraguay. Sentencia del 31 de agosto de 2004, Serie C Nº. 111, párr. 77; Caso "La Última Tentación de Cristo" (Olmedo Bustos y otros) Vs. Chile. Sentencia de 5 de febrero de 2001. Serie C Nº. 73, párr. 64; Corte I.D.H., La Colegiación Obligatoria de Periodistas (arts. 13 y 29 Convención Americana sobre Derechos Humanos). Opinión Consultiva OC-5/85 del 13 de noviembre de 1985. Serie A Nº. 5, párr. 30; CIDH. Informe Anual 1994. Capítulo V: Informe sobre la Compatibilidad entre las Leyes de Desacato y la Convención Americana sobre Derechos Humanos. Título III. OEA/Ser. L/V/II.88. doc. 9 rev. 17 de febrero de 1995; CIDH. Informe Nº. 130/99. Caso Nº. 11.740. Víctor Manuel Oropeza. México. 19 de noviembre de 1999, párr. 51; CIDH. Informe Nº. 11/96, Caso Nº. 11.230. Francisco Martorell. Chile. 3 de mayo de 1996. Párr. 53. Cita realizada por CIDH, Informe Nº 112/2012, Caso 12.828.

597 CIDH, Informe Nº 112/2012, Caso 12.828.

598 Cfr. Corte I.D.H., Caso Claude Reyes y otros. Sentencia de 19 de septiembre de 2006. Serie C Nº. 151, párr. 85; Corte I.D.H., Caso Herrera Ulloa Vs. Costa Rica. Sentencia de 2 de julio de 2004. Serie C Nº. 107, párr. 116; Corte I.D.H., Caso Ricardo Canese Vs. Paraguay. Sentencia del 31 de agosto de 2004. Serie C Nº. 111, párr. 86; Corte I.D.H., La Colegiación Obligatoria de Periodistas (arts. 13 y 29 Convención Americana sobre Derechos Humanos). Opinión Consultiva OC-5/85 del 13 de noviembre de 1985. Serie A Nº. 5, párr. 70. Cita realizada por CIDH, Informe Nº 112/2012, Caso 12.828.

599 CIDH. Alegatos ante la Corte Interamericana en el caso Ivcher Bronstein Vs. Perú. Transcritos en: Corte I.D.H., Caso Ivcher Bronstein Vs. Perú. Sentencia de 6 de febrero de 2001. Serie C Nº. 74, párr. 143. d); CIDH. Alegatos ante la Corte Interamericana en el caso "La Última Tentación de Cristo" (Olmedo Bustos y otros) Vs. Chile. Transcritos en: Corte I.D.H., Caso "La Última Tentación de Cristo" (Olmedo Bustos y otros) vs. Chile. Sentencia de 5 de febrero de 2001. Serie C Nº 73, párr. 61.b. Cita realizada por CIDH, Informe Nº 112/2012, Caso 12.828.

colectividad puedan desarrollarse plenamente. Es, en fin, condición para que la comunidad, a la hora de ejercer sus opciones, esté suficientemente informada. Por ende, es posible afirmar que una sociedad que no está bien informada no es plenamente libre"[600].

No cabe duda de la importancia que el derecho a la libertad de expresión y el acceso a la información, tiene para el desarrollo individual y colectivo, siendo fundamental para el efectivo goce de la libertad, de la democracia moderna y para la formación de opinión. Con el advenimiento de los nuevos servicios, cada vez se presentan más espacios e instancias que facilitan la libre expresión de las personas, así como el acceso a la información; siendo esencial garantizar estos derechos en todos los medios.

En este sentido, como surge de la Declaración Conjunta sobre Libertad de Expresión e Internet[601] del año 2011 (la "Declaración"): (i) la libertad de expresión es una herramienta esencial para la defensa de todos los demás derechos, como elemento fundamental de la democracia y para el avance de los objetivos de desarrollo sostenible; (ii) Internet, permite que miles de millones de personas en todo el mundo expresen sus opiniones, a la vez que incrementa significativamente su capacidad de acceder a la información, fomenta el pluralismo y la divulgación de información; (iii) Internet promueve y facilita la realización de otros derechos y la participación pública; (iv) algunos gobiernos han adoptado medidas con el objeto de restringir la libertad de expresión en Internet, en contravención al derecho internacional; (v) se reconoce que "*el ejercicio de la libertad de expresión puede estar sujeto a aquellas restricciones limitadas que estén establecidas en la ley y que resulten necesarias, por ejemplo, para la prevención del delito y la protección de los derechos fundamentales de terceros, incluyendo menores, pero recordando que tales restricciones deben ser equilibradas y*

600 Cfr. Corte IDH, La Colegiación Obligatoria de Periodistas (arts. 13 y 29 Convención Americana sobre Derechos Humanos). Opinión Consultiva OC-5/85 del 13 de noviembre de 1985. Serie A Nº. 5, párr. 70. Cita realizada por CIDH, Informe Nº 112/2012, Caso 12.828.

601 Relator Especial de las Naciones Unidas (ONU) para la Libertad de Opinión y de Expresión, la Representante para la Libertad de los Medios de Comunicación de la Organización para la Seguridad y la Cooperación en Europa (OSCE), la Relatora Especial de la Organización de Estados Americanos (OEA) para la Libertad de Expresión y la Relatora Especial sobre Libertad de Expresión y Acceso a la Información de la Comisión Africana de Derechos Humanos y de los Pueblos (CADHP). URL: http://www.oas.org/es/cidh/expresion/showarticle.asp?artID=849&lID=2 . Consultado el 20 de febrero de 2019.

cumplir con las normas internacionales sobre el derecho a la libertad de expresión"; (vi) preocupa que en ocasiones no se toman en cuenta las características de Internet y se restringe indebidamente la libertad de expresión.

En vista de lo anterior, en la Declaración se adoptaron los siguientes principios[602]:

a. La libertad de expresión se aplica a Internet del mismo modo que a todos los medios de comunicación.

b. Las restricciones a la libertad de expresión en Internet tienen una prueba tripartita: (1) deben estar previstas por ley, (2) deben perseguir una finalidad legítima, reconocida por el derecho internacional, y (3) tienen que ser necesarias para la finalidad.

c. Hay que evaluar la proporcionalidad de la restricción y diseñarse específicamente ateniendo las particularidades de Internet.

d. Ante contenidos ilícitos, deben desarrollarse enfoques que atiendan las particularidades de Internet y no deben establecerse restricciones especiales al contenido de lo que se difunde en Internet.

e. Se debe promover la autorregulación.

f. Fomentar la alfabetización digital, a fin de promover la capacidad de todas las personas de efectuar un uso autónomo, independiente y responsable de Internet.

En lo que respecta a la responsabilidad de los intermediarios, en la Declaración se señaló que por el principio de mera transmisión: *"Ninguna persona que ofrezca únicamente servicios técnicos de Internet como acceso, búsquedas o conservación de información en la memoria caché deberá ser responsable por contenidos generados por terceros y que se difundan a través de estos servicios, siempre que no intervenga específicamente en dichos contenidos ni se niegue a cumplir una orden judicial que exija su eliminación cuando esté en condiciones de hacerlo"*[603]. Además, se prevé que los intermediarios: (i) no deben ser responsables por los contenidos generados por terceros, (ii) no se les debe exigir que controlen el contenido generado por usuarios, y

602 Declaración Conjunta sobre Libertad de Expresión e Internet del año 2011, obra citada.
603 Declaración Conjunta sobre Libertad de Expresión e Internet del año 2011, obra citada.

(iii) no deben estar sujetos a normas extrajudiciales vinculadas a cancelar contenidos que no otorguen suficientes garantías a la libertad de expresión[604].

Asimismo, la Declaración dispone que:

i. el bloqueo de sitios web, direcciones IP, puertos, protocolos de red o de ciertos tipos de usuarios, constituye una medida extrema, análoga a la prohibición de un periódico o una emisora de radio o televisión, que solo podría justificarse conforme a estándares internacionales, como ser: proteger a menores del abuso sexual;

ii. el filtrado de contenido dispuesto por prestadores de servicios y/o por gobiernos, es una forma de censura previa, no justificada, que afecta a la libertad de expresión, si es que no puede ser controlado por los usuarios. Por lo que es importante informar la forma en que funcionan los filtrados, y las desventajas que puede haber en caso de que el filtrado sea excesivo[605].

En relación a las responsabilidades penales y civiles, la Declaración dispone que[606]:

i. Se debe prevenir el "turismo de la difamación", para lo cual: (a) debería ser competencia exclusiva de los Estados donde las causas presenten los contactos más estrechos, por ejemplo: que el autor resida en ese Estado, que el contenido se hubiere publicado desde allí y/o se dirija específicamente al Estado en cuestión, y (b) los particulares solo deberían poder iniciar acciones judiciales en la jurisdicción en la que puedan demostrar haber sufrido un perjuicio sustancial.

ii. Se debe preservar el "lugar público de reunión" que cumple Internet: para lo cual se debería tener en cuenta el interés general del público en proteger la expresión y el foro en el cual se pronuncia.

iii. Por la regla de "publicación única": en el supuesto de contenidos publicados con mismo formato y lugar, los plazos para iniciar acciones judiciales deberían correr desde la primera publicación. Además, debería presentarse una sola acción por los daños generados por dichos contenidos y una única reparación por los daños sufridos.

604 Declaración Conjunta sobre Libertad de Expresión e Internet del año 2011, obra citada.
605 Ibídem.
606 Ibídem.

En relación a la neutralidad de la red, la Declaración señala que[607] el "*tratamiento de los datos y el tráfico de Internet no debe ser objeto de ningún tipo de discriminación en función de factores como dispositivos, contenido, autor, origen y/o destino del material, servicio o aplicación*"; y que se debería exigir a los intermediarios de Internet que: (i) sean transparentes respecto a las prácticas para la gestión del tráfico o de la información, y (ii) que pongan a disposición del público información relevante sobre dichas prácticas.

Finalmente, en relación al acceso a Internet, la Declaración prevé, entre otras cosas, que los Estados tienen la obligación de promover el acceso universal a Internet para garantizar el derecho a la libertad de expresión, así como otros derechos, como ser: la educación, la salud, el trabajo; y que como mínimo deberían: (i) establecer mecanismos regulatorios para fomentar un acceso más amplio, (ii) facilitar el acceso al público, (iii) concientizar sobre el uso adecuado y sus beneficios, (iv) asegurar el acceso equitativo para personas con discapacidad y los menos favorecidos[608].

Por otra parte, cómo surge de los "*Estándares para una Internet Libre, Abierta e Incluyente*[609]*",* entre otras cosas, hay preocupación respecto a diversos bloqueos de sitios web o de aplicaciones específicas que algunos países han dispuesto, sin considerar el impacto de dichas medidas en la libertad de expresión. Como ejemplo, se señala que en Brasil se ordenó, en varias ocasiones, el bloqueo de Whatsapp porque, entre otras cosas, la empresa no cumplió con órdenes judiciales que le requerían datos de usuarios y acceso a comunicaciones. Al respecto, se destaca que resulta admisible la adopción de medidas obligatorias de bloqueo y filtrado de contenidos específicos, ante casos excepcionales, como es cuando se está frente a contenidos evidentemente ilícitos (por ejemplo: pornografía infantil) o ante discursos no resguardados por la libertad de expresión (por ejemplo: propaganda de guerra o apología al odio). Pero, incluso en estos casos, es fundamental que las medidas sean adecuadas, proporcionales, y que no afecten otros contenidos o discursos legítimos que merecen protección. Además, es importante que estas medidas sean la excepción, que se adopten solo cuando no hay otra forma de alcanzar la finalidad, y que haya salvaguardas que eviten abusos, como transparencia

607 Ibídem.
608 Ibídem.
609 Relatoría Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos, OEA: "Estándares para una Internet libre, abierta e incluyente". URL: http://www.oas.org/es/cidh/expresion/docs/publicaciones/INTERNET_2016_ESP.pdf Consultado el 20 de febrero de 2019.

respecto de los contenidos cuya remoción sea requerida, así como la necesidad y la justificación.

Considerando todo lo anterior, en el año 2015 se aprobaron los Principios de Manila sobre Responsabilidad de los Intermediarios[610], son una guía de buenas prácticas para delimitar la responsabilidad de los intermediarios de contenidos y para promover la libertad de expresión y la innovación. Los principios son los siguientes: (i) deben estar protegidos por ley de la responsabilidad por contenido de terceros; (ii) no deben ser obligados a restringir contenidos sin una orden emitida por una autoridad judicial; (iii) las solicitudes de restringir contenidos deben ser claras, inequívocas y respetar el debido proceso; (iv) las leyes, órdenes y prácticas de restricción de contenidos deben cumplir con los test de necesidad y proporcionalidad; (v) las leyes, políticas y prácticas de restricción de contenido deben respetar el debido proceso; (vi) la transparencia y la rendición de cuentas deben ser incluidas dentro de la normativa, políticas y prácticas sobre restricción de contenido.

En definitiva, teniendo en cuenta la importancia que la libertad de expresión tiene por sí misma, así como para garantizar el efectivo goce de otros derechos y libertades, es esencial considerar que[611]:

i. Cualquier restricción a este derecho debe demostrarse como necesaria y como el medio menos restrictivo, ateniendo los principios de necesidad y proporcionalidad.

ii. Como reconoció el Tribunal de Justicia de la Unión Europea, entre otras, en la sentencia dictada en el caso Satakunnan Markkinaporssi y Satamedia, este derecho no se limita a los medios tradicionales, Internet un medio de comunicación, no siendo determinante el soporte en el que se transmiten los datos.

iii. Como señaló el Tribunal Constitucional de España, constituye censura previa: *"cualesquiera medidas limitativas de la elaboración o difusión de una obra del espíritu, especialmente al hacerlas depender del previo examen oficial de su contenido"*[612].

610 Principios de Manila sobre Responsabilidad de los Intermediarios. URL: https://www.eff.org/files/2015/06/23/manila_principles_1.0_es.pdf . Consultado el 20 de febrero de 2019.

611 SIGÜENZA, ALICIA: "La libertad de expresión en Internet" en *El Derecho de Internet*, Atelier Libros Jurídicos. Barcelona, 2016. pp. 57 y ss.

612 El Tribunal Constitucional de España en Sentencia 52/1983, RTC 1983/52.

iv. En lo que respecta a la responsabilidad de los intermediarios, la Directiva 2000/31/CE del Parlamento Europeo y del Consejo, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico, prevé en su artículo 15 que los Estados no impondrán a los prestadores de servicios una obligación general de supervisar los datos que transmitan o almacenen, ni de realizar búsquedas activas de hechos o circunstancias de actividades ilícitas.

Sobre este punto el Tribunal de Justicia de la Unión Europea "*en sentencia de 24 de noviembre de 2011 en el caso C-70/10 Scarlet Extended SA contra SABAM*[613] *(...) afirma que el artículo 15 prohíbe rotundamente a las autoridades nacionales adoptar medidas que obliguen a un operador de Internet a proceder a una supervisión general de los datos que transmite en su red o a realizar búsquedas activas de hechos o circunstancias que indiquen actividades ilícitas. Dicha sentencia también advierte de que las medidas de filtrado pueden implicar una vulneración sustancial de la libertad de empresa, dado que obligarían a establecer un sistema complejo, gravoso, permanente y exclusivamente a expensas del intermediario, así como una vulneración del derecho a la información. Este criterio ha sido confirmado en la sentencia del TJUE de 16 de febrero de 2012 en el asunto C-360/10, SABAM v. Netlog NV.*[614]"

Mas, como señala la Directiva, si el prestador de servicios colabora con uno de los destinatarios de su servicio para cometer actos ilegales, va más allá de lo que es la mera prestación de servicios y no puede beneficiarse de las exenciones de responsabilidad. Asimismo, las limitaciones de la responsabilidad no afectan la posibilidad de que se entablen acciones de cesación, como puede ser que se ponga fin a cualquier infracción, que se retire información ilícita o que se imposibilite el acceso a ella. Para tener la responsabilidad limitada, el prestador de servicios debe actuar con prontitud, en cuanto tenga *conocimiento efectivo* de la actividad ilícita[615].

---

613 STJUE en el caso c-70/10, Scarlet Extended SA y Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM), de 24 de noviembre de 2011. Citado por SIGÜENZA FLÓREZ, A.: "La libertad de expresión en Internet" en *El Derecho de Internet*, Atelier Libros Jurídicos, año 2016.

614 STJUE en el caso C-360/10, SABAM y Netlog NV, de 16 de febrero de 2012. Citado por SIGÜENZA, ALICIA, obra citada, pp. 57 y ss.

615 Considerandos 44 a 46 de la Directiva 2000/31/CE del Parlamento Europeo y del Consejo de 8 de junio de 2000 relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior (Directiva sobre el comercio electrónico).

Se considera que un prestador tiene conocimiento efectivo, cuando un órgano competente: (i) dicte resolución: (ii) declare la ilicitud, (iii) ordene el retiro o la imposibilidad de acceder a los mismos o se declare la existencia de lesión, y (iv) el prestador conozca dicha resolución.[616]

En los hechos, el contenido se puede restringir, tanto por ley como por autorregulación o políticas privadas de las compañías, como pueden ser los términos y condiciones de uso. Al respecto, es importante que las políticas privadas o los términos y condiciones de uso sean claros, transparentes, que prefijen el tipo de contenido no deseado, que podría ser removido, los criterios que se consideran, la forma en que se implementa y si el usuario tiene algún recurso. Asimismo, es importante que no se encubran prácticas discriminatorias o que puedan afectar los derechos humanos. Finalmente, considerando la naturaleza universal de Internet, sería deseable alcanzar uniformidad en la responsabilidad a fin de dar garantías y mantener una Internet, abierta, libre y global[617].

En suma, gracias a Internet y a las plataformas, las personas tienen más posibilidades de expresarse libremente, de compartir y generar información y contenido, así como de acceder a él. Es fundamental garantizar y potenciar estos derechos y libertades, en todas sus modalidades, en tanto son derechos esenciales para el desarrollo de todos los individuos, de la opinión pública, así como para la existencia de una sociedad libre.

En lo que respecta a sus límites, se debe buscar el adecuado equilibrio y la proporcionalidad, y realizar la prueba tripartita: (1) previsto por ley, (2) perseguir una finalidad legítima, reconocida por el derecho internacional, y (3) tienen que ser necesarias para la finalidad.

A continuación se procede a desarrollar sobre los discursos de odio y la moderación de contenidos, es un desafío muy actual, dado que se debe mover en una línea muy fina para no afectar o limitar derechos. A estos efectos, se hará mención específica al régimen de Estados Unidos y se desarrollará en el idioma inglés.

---

616 Sigüenza, Alicia, obra citada, pp. 57 y ss.

617 Comisión Interamericana de Derechos Humanos en *Estándares para una Internet Libre, Abierta e Incluyente.*

(III.1) Hate speech and Content Moderation.

(III.1.A) Introduction

Content moderation practices in cyberspace are needed. Otherwise, we would be full of spam, traumatizing content, disturbing images, and information that can encourage bad behavior at the time that may discourage people from using online platforms and may affect the trust in the digital world.

Nowadays, cyberspace is an important place where we can exchange views and is seen as the leading democratic forum.

First Amendment protects freedom of speech, and Section § 230 immunizes online platform for what users post and allow them to restrict some content.

Hate speech is a kind of speech which is protected by the First Amendment, some platform can download it, but others not. Considering how that type of content may affect the internet forum is critical to consider if it must be blocked or restricted.

The issue is that online platforms may use intelligent systems to control their platforms. Still, those systems may over-block or under-block, and also is not the same the reality of big platform rather than the possibilities that small platforms have.

I think that the situation requires a more in-depth analysis, looking for a balance, and working together in a multistakeholder ecosystem.

(III.1.B) Freedom of Speech

The Constitution of the United States sets in the First Amendment: *"Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances."*

There is no doubt that the First Amendment has to be also applied in the online world. In this sense, *See Packingham v. North Carolina:* "A fundamental principle of the First Amendment is that all persons have access to places where they can speak and listen, and then, after reflection, speak and listen once more." (…) "Even in the modern era, these places are still essential venues for public gatherings to celebrate some views, to protest others, or simply to learn and inquire.

While in the past, there may have been difficulties in identifying the most important places for the exchange of views; today, the answer is clear. It is cyberspace – the "vast democratic forums of the Internet" in general, *See Reno v. American Civil Liberties Union*, 521 U.S. 844, 868 (1997), and social media in particular. Seven in ten American adults use at least one Internet social networking service. One of the most popular of these sites is Facebook, the area used by the petitioner, leading to his conviction in this case. According to sources cited to the Court in this case, Facebook has 1.79 billion active users. This is about three times the population of North America." (…)

"Social media allows users to gain access to information and communicate with one another about it on any subject that might come to mind. By prohibiting sex offenders from using those websites, North Carolina with one broad stroke bars access to what for many are the principal sources for knowing current events, checking ads for employment, speaking and listening in the modern public square, and otherwise exploring the vast realms of human thought and knowledge. These websites can provide perhaps the most powerful mechanisms available to a private citizen to make his or her voice heard. They allow a person with an Internet connection to "become a town crier with a voice that resonated farther than its could from any soapbox" Reno, 521 U.S., at 870.[618]"

Also is clearly that "When the government provides a forum for speech (known as a public forum), the government may be constrained by the First Amendment, meaning that the government ordinarily may not exclude speech or speakers from the forum on the basis of viewpoint…", see Manhattan Community Access Corp. et. Al. v. Hallech et al, 587 U.S. (2019).

Nonetheless, as Professor James Grimmelmann teaches, there is some harmful speech that is not protected. In this sense, the Supreme Court has recognized a close list of "several types of unprotected speech, which typically combine serious harms with few offsetting benefits for society[619]". For example:

[618] GRIMMELMANN, JAMES, Internet Law, Semaphore Press, 2019. pp. 122 y ss.
[619] Obra citada, pp . 142-184.

Violent speech: true threats judged by a reasonable person, i.e., "unequivocal, unconditional and specific expressions of intention immediately to inflict injury". See United States v. Kelner[620].

Speech integral to planning the commitment of criminal conduct, see Giboney v. Empire Storage & Ice Co., 336 U.S. 490 (1949)[621].

False speech if there is harm associated. See States v. Alvarez, 567 U.S. 709, 719 (2012)[622].

Defamation: there are some limits considering, among other things, if the plaintiff is a public figure. See Gertz v. Robert Welch, Inc., 418 U.S. 323, 351 (1974), also if he or she has shown actual malice. See New York Times Co. v. Sullivan, 376 U.S. 254 (1964). See Dun & Bradstreet, Inc. V. Greenmoss Builders, Inc., 472 U.S. 749, 759 (1985)[623].

Invasion of Privacy: matters of public concern are at the heart of the protection. See Gawker Media, LLC v. Bollea. 129 So. 3d 1196 (Dist. Ct. App. Fla. 2014).[624] Impersonation: when someone impersonates another to cause injury, harm reputation of another, or the intent to interfere with governmental operations. See People v. Golb [Golb I][625].

Harassment: Restatement (second) of torts [emotional distress] 46 outrageous Conduct Causing Severe Emotional Distress: (1) One who by extreme and outrageous conduct intentionally or recklessly causes severe emotional distress to another is subject to liability for such emotional distress, and if bodily harm to the other results from it, for such bodily harm.[626]

was at a public place on a matter of public concern, that speech is entitled to "special protection" under the First Amendment. Such speech cannot be restricted simply because it is upsetting or arouses contempt. If there is a bedrock principle underlying the First Amendment, it is that the government may not prohibit the

[620] Obra citada, pp . 142.
[621] Obra citada, pp . 148.
[622] Obra citada, pp . 153.
[623] Obra citada, pp . 153.
[624] Obra citada, pp . 155.
[625] Obra citada, pp . 162.
[626] Obra citada, pp . 166.

expression of an idea simply because society finds the idea itself offensive or disagreeable. Texas v. Johnson, 491 U.S. 397, 414 (1989).

Harm to minors: See Brown v. Entertainment Merchants Ass'n. 564 U.S.786, (2011). "California correctly acknowledges that video games qualify for First Amendment protection. Like the protected books, plays, and movies that preceded them, video games communicate ideas – and even social messages through many familiar literary devices (such as characters, dialogue, plot, and music) and features distinctive to the medium (such as the player's interaction with the virtual world). That suffices to confer First Amendment protection[627].

Pornography: there are three categories of harmful speech: (1) obscenity: Miller v. California, 413 U.S.15(1973): "(a) whether the average person, applying contemporary community standards would find that the work, taken as a whole, appeals to the prurient interest; (b) whether the work depicts or describes, in a patently offensive way, sexual conduct specifically defined by the applicable state law; and (c) whether the work, taken as a whole, lacks serious literary, artistic, political, or scientific value". (2) child pornography: children engaging in sexual acts can be prohibited outright, and mere possession of it is criminal. (3) material for adults that can be harmful to minors. FCC v. Pacific Found, 438 U.S.726(1978)…admonished that "the fact that society may find speech offensive is not a sufficient reason for suppressing it". Id. At 745.[628]

(III.3.C) Statutory Immunity, section § 230

As a way to protect online platforms and telecommunication companies from responsibility for the content posted by users, a statutory immunity was approved under section § 230; the main goal was to protect innovation.

In this sense, considering the fast development of Internet and interactive computer services, which are available for everyone, an educational and informational resource for everyone, a forum for diversity, and an avenue to develop culture and intellectual activity, being beneficial for all American, with a minimum of government regulation.

Additionally, in light of Americans relayed on interactive media for a variety of political, educational, cultural, and entertainment services; the policy of the United

[627] Obra citada, pp . 171.
[628] Obra citada, pp . 178 y ss.

States is to promote the development of the Internet and other interactive computer services, to preserve the competition, to encourage the development of technologies which maximize user control over what information is received society, to remove disincentives for the development and utilization of blocking and filtering technologies that empower parents to restrict their children's access to objectionable or inappropriate online material; and to ensure enforcement of Federal criminal laws to deter and punish trafficking in obscenity, stalking, and harassment by means of a computer.

Regarding the above mentioned, the protection for "Good Samaritan", states that:

the provider of interactive computer services may not be treated as the publisher or speaker of any information provided by users.

Protect interactive computer service for responsibility for any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected; or for any action to restrict access to material described.

Nonetheless, for this, the interactive computer service, at the time to start a relationship with the customer may inform customers that parental control protections (such as computer hardware, software, or filtering services) are commercially available which may help customers in restrict access to material that may be harmful to minors.

It is important to remark that, as the Congress mentioned, Pub. L 115-164, Apr. 11, 2018, 132 Stat. 1253, section § 230 "was never intended to provide legal protection to websites that unlawfully promote and facilitate prostitution and websites that facilitate traffickers in advertising the sale of unlawful sex acts with sex trafficking victims". Neither too "websites that promote and facilitate prostitution have been reckless in allowing the sale of sex trafficking victims and have done nothing to prevent the trafficking of children and victims of force, fraud, and coercion". So in 2018, they added a clarification to ensure that does websites are not protected.

As it is set in Zeran v America Online, Inc.: "By its plain language, 230 creates a federal immunity to any cause of action that would make service providers liable for information originating with a third-party user of the service. (…)

The purpose of this statutory immunity is not difficult to discern. Congress recognized the threat that tort-based lawsuits pose to freedom of speech in the new and

burgeoning Internet medium. The imposition of tort liability on service providers for the communications of others represented, for Congress, simply another form of intrusive government regulation of speech. Section 230 was enacted, in part, to maintain the robust nature of Internet communication and, accordingly, to keep government interference in the medium to a minimum. In specific statutory findings, Congress recognized the Internet and interactive computer services as offering "a forum for a true diversity of political discourse, unique opportunities for cultural development, and myriad avenues for intellectual activity"[629].

The purpose of the immunity considered that it is not possible to screen all of the million posts done by the millions of users, which can be millions of potential problems, so If service providers were liable for their content, they would choose to restrict them. Also, they encourage service providers to self-regulate the dissemination of offensive material over their services, but if they regulate the dissemination of offensive material on their services, they may be subjected to liability as a publisher. At the same time, if they are subject to distributor liability, they may be responsible each time they receive notice of any message that potentially can be defamatory

Considering the above said, the courts have been interpreting section § 230 broadly, but it is not without limits.

See Jones v. Dirty World Entertainment Recordings LLC. 755 F. 3d 398 (6TH Cir. 2014). "Section 230 (c)(1)'s the grant of immunity is not without limits, however. It applies only to the extent that an interactive computer service provider is not also the information content provider of the content at issue. An " information content provider" is defined as "any person or entity that is responsible, in whole or in part, for the creation or development of information provided through the Internet or any other interactive computer service." 47 U.S.C. 230(f) (3). A website operator can simultaneously act as both a service provider and a content provider. If a website displays content that is created entirely by third parties, then it is only a service provider concerning that content – and thus is immune from claims predicated on that content. However, if a website operator is in part responsible for the creation or development of content, then it is an information content provider as to that content – and is not immune from claims predicated on it. Thus, a website may be immune from liability for some of the third-party content it publishes but be subject to liability for the content that it is

[629] Obra citada, pp . 188 y ss.

responsible for as a creator or developer. In short, immunity the CDA depends on the pedigree of the content at issue."[630]

As we mentioned above, the First Amendment prohibits the government from restricting speech, except specific cases, that may be happening through tech companies when they moderate intentionally or not the content. Nonetheless, tech companies are allowed to create rules that moderate the content on their platform, and at the same time, if the government regulates the rules that those platforms must follow at the time to moderate the content, the First Amendment may be affected.

Online platforms may not be liable for the content posted by users. Nonetheless, they are responsible for what they do, such as moderate the content, clarify the rules used, and no discriminate.

(III.3.D) Content Moderation

Today in many cases we do not know the rules followed by the algorithm, which are designed and coded by humans, run by computers automatically, made a recommendation based on filtering results, affecting in some way the information that people is going to see, and using this way to show more ads and sell more.

The systems are very intelligent and are enriched by people's data, e.g., peoples use, but many companies protected them as a trade secret, and the results can be hazardous. For example, as the New York Times reported, the algorithm of a specific social network was encouraging pedophiles to watch videos of children partially-clothed, incentivizing lousy behavior. *"Human intuition can recognize in people's viewing decisions and can step in to discourage that – which most likely have happened if human, and not a computer were recommending videos. But to (...) nuance-blind algorithm – trained to think with simple logic- serving up more videos to state a sadist's appetite is a job well done"*[631].

Recently Chris Stokel-Walker wrote an article named[632] "*As humans go home, Facebook and Youtube face a coronavirus crisis."* In this article, we can see how

---

[630] Obra citada, pp . 199 y ss.

[631] New York Times, Chris Stokel-Walker: "Algorithms Won't Fix What's Wrong With Youtube" https://www.nytimes.com/2019/06/14/opinion/youtube-algorithm.html?auth=login-email&login=email.
Search: may 13th 2020.

[632] Chris Stokel-Walker, https://www.wired.co.uk/article/coronavirus-facts-moderators-facebook-youtube Search: may 13th 2020.

artificial intelligence systems are replacing human to moderate content. However, now it is essential because workers that moderate and monitor content on social networks for their safety have to be at home during the spread of the coronavirus, and in some cases, through contractual restrictions, they could not do their job from their homes.

The workers that moderate and monitor content on social networks are the ones who filter and block content and define if it is acceptable or not, in light of the rules of the specific website, maintaining them accessible and relatively clean.

The issue now is that workers have to be at home; artificial intelligence systems are the ones who are doing all the job. Workers and artificial intelligence have been working together for many years, but now those systems are more useful than ever and are doing almost all the job and the risk of over-blocking that it was simple to visualize how it is proved.

Although social networks are not governmental actors and they are relieved from formal constitutional concerns about content restrictions, it is easier to see that they have a substantial influent and power over the public. In some way they are setting policies that discretionally can affect and censor people's lives. It is essential to control potential abuses.

In this line, the main problem related to free speech is to be aware and not allow new technologies to betray its values. Online platforms and speed of communications make control challenging to implement and hard to protect constitutional values. Even though it is necessary to take hard, fast, and specific decisions to control bad actors that can affect peoples' rights, mandatory models may require platforms to protect free speech standards by ensuring transparency disclosing content moderation policies and procedures, and defining the set of users' rights.

(III.3.E) Challenges

Currently, we are suffering a global pandemic, and among other issues, it is disclosing some realities that we all know, but now their importance increased exponentially.

As an example, recently, YouTube declared: *"Our Community Guidelines enforcement today is based on a combination of people and technology: Machine learning helps detect potentially harmful content and then sends it to human reviewers for assessment. As a result of the new measures we are taking, we will temporarily start*

relying more on technology to help with some of the work normally done by reviewers. This means automated systems will start removing some content without human review, so we can continue to act quickly to remove violative content and protect our ecosystem, while we have workplace protections in place.

As we do this, users and creators may see increased video removals, including some videos that may not violate policies. We won't issue strikes on this content except in cases where we have high confidence that it's violative. If creators think that their content was removed in error, they can appeal the decision and our teams will take a look. However, note that our workforce precautions will also result in delayed appeal reviews. We'll also be more cautious about what content gets promoted, including livestreams. In some cases, unreviewed content may not be available via search, on the homepage, or in recommendations.[633] "

It is noble that they clearly show how they are doing the moderation, but it is remarkable that they recognized that:

- the content filtered can be "potentially" harmful,
- they are relying more on technology to do work that usually is done by humans,
- an automated system will start removing some content,
- they are acting quickly to remove violative content to protect the ecosystem,
- users and creators may see increased content removal.

That is only an example, but the same is happening with other platforms. For instance, anti-spam filters used by Facebook are more aggressive now, and in some cases, people who tried to share new stories and information related to coronavirus could not be posted them because of anti-spam rules[634].

Recently Mark Zuckerberg said that the basis of all the work is misinformation specifically hate speech which could incite violence and that they never allowed things

[633] YouTube: https://youtube-creators.googleblog.com/2020/03/protecting-our-extended-workforce-and.html?m=1
Search: may 13th 2020.

[634] STOKEL-WALKER, CHRIS, https://www.wired.co.uk/article/coronavirus-facts-moderators-facebook-youtube
Search: may 13th 2020.

that would be an imminent physical risk and "Even in the most free-expression, friendly traditions like the United States, you've long had the precedent that you don't allow people to yell fire in a crowded room, and that – I think it's similar to people spreading dangerous misinformation in the time of an outbreak like this."[635]

In these lines Stokel-Walker affirmed that "It's better to accidentally suppress the spread of "good" information in order to ensure "bad" information absolutely can't take a foothold".

However, the issue, as Frederick Kaltheuner, from Mozilla, said is that "manual flagging mechanisms are also often abused by people who engage in coordinated flagging to contents", and automated systems just follow those decisions or in some cases, the own systems are learning from the data and are making their own decision.

With the pandemic, everything is easy to visualize. The risk of using artificial intelligence is that filters cannot distinguish legal from illegal content, code is a type of language and behind them are people who are making the decision or at least the first one, and by error or not, consciousness or not, they can be discriminating, affecting free speech and access to information.

As we will mention, freedom of speech is one of the main values of the United States, and the Section § 230protects online platforms from de dissemination of content. But, in the new reality in which we are living, it is essential to protect the freedom of speech as one of the main values.

(III.3.F) What is happening with hate speech?

According to Cambridge Dictionary, "Hate Speech" is any "public speech that expresses hate or encourages violence toward a person or group based on something such as race, religion, sex, or sexual orientation[636]"

There is a severe concern about hate speech because of the consequence and the harm that it can generate, but as a kind of speech it is protected by the First

---

[635] https://about.fb.com/wp-content/uploads/2020/03/March-18-2020-Press-Call-Transcript.pdf Search: may 13th 2020.

[636] Cambridge Dictionary, https://dictionary.cambridge.org/dictionary/english/hate-speech [20] https://www.nytimes.com/2019/08/06/technology/section-230-hate-speech.html Search: may 13th 2020.

Amendment, and citizens require that online platforms should take actions to remove this content, but they do not have a responsibility because of section § 230.

In 2019 two shootings occurred in the United States, and in both the responsible posted hate speech manifestos in a service provider, which was favorable to that content[637].

Could be different if that platform had blocked o filtered that content?

Some think that yes, and some congress members are analyzing to pass a law to change Section § 230 to make service providers liable for hate speech in order to block or filter them. Nonetheless others consider that the restriction can be done using other acts without changing the section § 230[638]

There are different realities with online platforms. On the one hand, there are big platforms such as Facebook or Google, then can quickly develop an algorithm able to filter or block some content, with the risk to over-block. Moreover, on the other hand, there are small platforms, some specialized in specific topics, that may do not have possibilities to develop complex algorithms and can be under blocking or directly they are not able to comply with new obligations affecting diversity, competition, freedom of speech and access to information.

In this sense, it is important to consider the role that the platform has in the content, if it intentionally encourages illegal or actionable third-party postings or if they are editorially neutral and have the immunity for content posted by users.

See Cyber Promotions, Inc v. American Online, Inc 948F. Supp. 436 (E.D.Pa. 1996): "Whether Cyber has a right under the First Amendment of the United States Constitution to send unsolicited e-mail to AOL members via the Internet and concomitantly whether AOL has the right under the First Amendment to block the e-mail sent by Cyber from reaching AOL members over the Internet…"[639]

"The First Amendment to the United States Constitution states that "Congress shall make no law respecting an establishment of religion, or prohibiting the free

[637] https://www.nytimes.com/2019/08/06/technology/section-230-hate-speech.html Search: may 13th 2020.

[638] https://www.bloomberg.com/news/features/2019-08-07/section-230-was-supposed-to-make-the-internet-a-better-place-it-failed Search: may 13th 2020.

[639] GRIMMELMANN, JAMES, Internet Law, Semaphore Press, 2019. pp. 529.

exercise thereof; or abridging the freedom of speech, or of the press." The united States Supreme Court has recognized that "the constitutional guarantee of free speech is a guarantee only against abridgement by government, federal or state". Hudgens v. NLRB, 424 U.S. 507, 513 (1976) Only recently, the Supreme Court has stated that "the guarantees of free speech… guard only against encroachment by the government and erect no shield against merely private conduct." Hurley v. Irish-American Gay Group of Boston, 515 U.S. 557, 566 (1995)[640].

"As a result, tens of millions of people with access to the Internet can exchange information. AOL is merely one of many private online companies that allow its members access to the Internet through its e-mail systems where they can exchange information with the general public. The State has absolutely no interest in, and does not regulate, this exchange of information between people, institutions, corporations, and governments around the world[641]".

In this sense, it is essential to remark that AOL is a service provider that opened its services to everyone, but they are not performing any essential or public service; they are not part of the Government, they are just a private actor, providing a service.

See Zhang b. Baidu.com Inc., 10 F. Supp. 3d 433 (S.D.N.Y. 2014): "The case raises the question of whether the First Amendment protects as speech the results produced by an Internet search engine. The court concludes that, at least in the circumstances presented here, it does.[642]" "Here, the very theory of Plaintiffs' claims is that Baidu exercises editorial control over its search results on certain political topics – namely, by disfavoring expression concerning "the Democracy movement in China" and related subjects. In other words, Plaintiffs do not -and, in light of their own allegations, cannot – make any argument that Baidu is merely an "infrastructure or platform that delivers content" in a neutral way. (…) Instead, they seek to hold that Baidu liable for, and thus punish Baidu for, a conscious decision to design its search-engine algorithms to favor certain expression on core political subjects over other expression on those same political subjects. To allow such a suit to proceed would plainly "violate the fundamental rule of protection under the First Amendment, that a

[640] Obra citada, pp . 530.
[641] Obra citada, pp . 531.
[642] Obra citada, pp . 533.

speaker has the autonomy to choose the content of his own message" Hurley, 515 US at 573.(….)

"It is debatable whether any search engine is a mere "conduit" given the judgements involved in designing algorithms to choose, rank, and sort search results. But whether or not that proposition is true as a general matter, it is plainly "not apt here", as Plaintiffs' own allegations of censorship make clear that Baidu is "more than a passive receptacle or conduit for news, comment, and advertising". Hurley, 515 U.S. at 575 . As Plaintiffs themselves allege, for example, Baidu "purposely designs its search engine algorithms to exclude any pro-democracy topics, articles, publications, and multimedia coverage[643]".

Even the above mentioned, It is interesting to mention that the Court understood that the option of Baidu to not show some features is part of their freedom and protected by the First Amendment.

In the same way, in Marshall's Locksmith Service Inc. v. Google, LLC F3d, 2019 WL 2398008 (D.C. Cir. June 7, 2019): "… the defendants use automated algorithms to convert third-party indicia of location into pictorial form. Those algorithms are "neutral means" that do not distinguish between legitimate and scam locksmiths in the translation process[644]"

Considering the above said, platforms are private actors who have the right to develop their algorithm and display the result that they preferred to, as part of their freedom of speech, is protected by the First Amendment, and being able to be considered neutral.

Also, applying platforms have the good Samaritan protection that allows them to block and screen, being able also to restrict access to or availability of material that the provider considers being obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected.

See Song Fi, Inc v. Google, Inc. 108 F. Supp. 3d 876 (N.D. Cal. 2015): "Congress did not define the phrase "otherwise objectionable", the Court follows the common practice of consulting dictionary definitions… The dictionary definition of the term

[643] Obra citada, pp . 537.
[644] Obra citada, pp . 542.

"objectionable" at the time Congress enacted the Communications Decency Act was "undesirable, offensive". Webster's Ninth New Collegiate Dictionary 814 (9TH ED. 1984).

Nevertheless, the meaning is not determined in the abstract, and the Court must look to whether these definitions are consistent with the context of the Communications Decency Act.[645]"

The main concern is that many believe that platforms may do more and should remove some content such as those linked with hate speech because propagate of that content can affect citizens. Other are afraid if in doing that part of their ideas or expression are removed or censorship point of views also.

Both positions are reasonable, the issue is that everything is changing very fast, technology has a limitation, and it is essential to attend proportionality, transparency, the necessity, the context, and that It is not the same if the platforms are specific or focus in a matter rather than if it is a general forum.

In this sense, there is no doubt that hate speech can damage harmony and cohabitation rules. Nonetheless, set general rules maybe not contemplate specific cases, and specific rules at the same time can damage core values.

Balance is the key, and the central aspect is to ask the platform to be transparent and clear about their term of use, making it possible for everyone to understand if they are filtering or blocking content, what kind, and how they are doing it.

In case the government wants to block specific content, as they did with FOSTA and child pornography. It is essential to well-defined that content, being proportional, and considering the necessity, giving certainly to internet companies and the public.

Platforms are indeed global, but using technology, they can generate different rules or codes considering the place and cultural values. Also, there will be an error at the time to moderate, but it can be fit and also informed in advance, being transparent and accountable.

(III.3.G) Conclusions

Freedom of speech and access to information is a core value worldwide.

[645] Obra citada, pp . 544.

First Amendment protects the freedom of speech.

Section 230 provides digital platforms immunity for users' posted and allow them to restrict some.

Hate speech is a big problem, and society requests a solution.

There are different ways to act to resolve this issue and to moderate content considering all the risks. The main aspects are transparency, proportionality, necessity, and procedural fairness.

Everything is changing very fast, technology has limitations, and the balance is the most important. Listen and work together with all the stakeholders, seems to be the best solution. A hard decision can affect other values, and also the potential competition in the market.

Overall, it is essential to make a change in section 230 right now. We should continue analyzing, working together, and try to set principles that have to follow and respect for all.

IV. El Derecho de Autor

(IV.1) Introducción

El diccionario de la Real Academia Española define a la "Propiedad Intelectual" como el *"Derecho de explotación exclusiva sobre las obras literarias o artísticas, que la ley reconoce a su autor durante un cierto plazo"*[646]; y al "Derecho de autor" como el "*derecho que la ley reconoce al autor de una obra intelectual o artística para autorizar su reproducción y participar en los beneficios que esta genere*"[647].

En este sentido, como señala la Organización Mundial de la Propiedad Intelectual (OMPI), la PI se relaciona con las creaciones de la mente, como pueden ser: las invenciones, las obras literarias y artísticas, los símbolos, nombres e imágenes utilizados en el comercio. Se intenta proteger esas creaciones, a fin de fomentar la

[646] Diccionario de la Real Academia Española, URL: https://dle.rae.es/propiedad Consultado el 18 de diciembre de 2019.
[647] Diccionario de la Real Academia Española, URL: https://dle.rae.es/derecho#CUr4nPg Consultado el 18 de diciembre de 2019.

creatividad y la innovación, a través de diversas modalidades como pueden ser las patentes, los derechos de autor y las marcas[648].

Está reconocido en el artículo 27.2 de la Declaración Universal de Derechos Humanos en tanto dispone que: *"Toda persona tiene derecho a la protección de los intereses morales y materiales que le correspondan por razón de las producciones científicas, literarias o artísticas de que sea autora."*, y en el Artículo 17.2 de la Carta de Derechos Fundamentales de la Unión Europea. Sin perjuicio, su primer reconocimiento fue en el Convenio de París, para la protección e la Propiedad Industrial del año 1883, y en el Convenio de Berna para la Protección de las Obras Literarias y Artísticas del año 1886.

En esta línea, se diferencia por un lado a la propiedad industrial, que engloba lo referente a las patentes, las marcas, los diseños industriales y las indicaciones geográficas; y por otro lado, el derecho de autor, que comprende a las obras literarias, las películas, la música, las obras artísticas y los diseños arquitectónicos, entre otros.[649] Las ideas no son protegidas por la PI.

A los efectos del presente trabajo, nos enfocaremos en lo referente a los derechos de autor.

(IV.2) Orígenes

Si bien su protección es de larga data, uno de los factores determinantes fue la creación de la imprenta, en tanto *"...marcó el inicio de un fenómeno que alteraría sustancialmente la vida cotidiana del ser humano. Modificó la relación de la humanidad con su historia y su cultura, facilitó la expansión del libro y jugó un papel fundamental en la alfabetización de la gente. En adelante, los pensamiento de muchas personas perdurarían objetivados en libros. La imprenta permitió, también, acercar el conocimiento de las costumbres, expresiones artísticas y modos de vida – de la cultura- de unas naciones a otras, disminuyendo la distancia de países geográfica y culturalmente muy lejanos. Si la escritura determina el inicio de la historia (en contraposición a la prehistoria), la imprenta posibilitó, de una forma imposible hasta entonces, la difusión y reproducción del pensamiento humano escrito. Precisamente esa*

[648] OMPIhttps://www.wipo.int/about-ip/es Consultado el 14 de enero de 2020.
[649] OMPI: ¿Qué es la Propiedad Intelectual?. URL: https://www.wipo.int/edocs/pubdocs/es/intproperty/450/wipo_pub_450.pdf Consultado el 14 de enero de 2020.

difusión y reproducción (de pensamientos, de expresiones, de arte…) ha sufrido, con la informática e internet, un cambio de una magnitud nada desdeñable (a la altura o no de la imprenta es algo que historiadores futuros tendrán que valorar).

El siglo XIX, (…), adaptó el funcionamiento de la imprenta a las necesidades comerciales de un capitalismo en plena expansión, que poco a poco iba abarcando todos los aspectos de la vida humana en las sociedades occidentales (principalmente en Europa y Estado Unidos). Pero la obra cultural (el libro, la pintura, la composición musical, etc.) ha tenido siempre una suerte de doble naturaleza que vuelve compleja su adaptación al mundo comercial. Ello se debe a la propia condición del bien, al que la legislación se ha adaptado solo parcialmente. Así, se suele distinguir respecto de una obra artística el corpus mysticum, aquello que conforma la obra intelectual como ente abstracto, y el corpus mechanicum, representado por la plasmación física de tal obra[650]*."*

Sin duda la imprenta marcó un antes y un después en la historia mundial, permitiendo la transmisión y facilitando la creación, en tanto se podría trabajar sobre lo que otros ya habían creado, no teniendo que comenzar los análisis y estudios desde cero. Pero además, esta protección también respondió a las necesidades de la economía y de la sociedad, en tanto la creación, como la impresión, requerían recursos (tiempo y dinero) que tenían que ser protegidos a fin de justificar las inversiones.

Así *"Uno de los cambios sustanciales del siglo XIX fue, se ha dicho, la adaptación del funcionamiento de la imprenta a las necesidades del comercio del libros. Así, el siglo XIX protegió a los propietarios de las imprentas (y de los manuscritos) otorgándoles, mediante las primeras leyes de copyright, derecho de propiedad sobre la obra creada, de la que el autor se veía desposeído si quería poder imprimirla y ofrecerla al público. Estas primeras normas establecían un límite efectivo al uso de la imprenta; este invento revolucionario iba a servir para la difusión cultural, si, pero a condición de que existiera un beneficio económico para quien se pudiera permitir poseer la máquina y el manuscrito"*[651] *(…)*

[650] BRCOVITZ, RODRIGO, Manual de propiedad intelectual, Tirant lo Blanch, Valencia, 2012, pp. 19 Citado por RAMOS TOLEDANO, JOAN en Propiedad Digital, la cultura en Internet como objeto de cambio, Editorial Trotta, 2018, Madrid, España, pp. 47.
[651] Ibídem, pp. 49.

"La nueva sociedad capitalista se adaptó así a esta nueva situación de la producción cultura. Poseer una imprenta, comprar manuscritos y reproducirlos en esas máquinas para su posterior venta no se veía muy distinto a comprar telas y maquinaria y emplear trabajadores para la producción textil, vendiendo posteriormente el producto. La venta de este nuevo producto – el libro -, no obstante, no estaba exenta de problemas, pues otro editor podía, sin haber pagado por el manuscrito ni haber satisfecho cantidad alguna al autor, comprar un ejemplar del libro e imprimirlo en su imprenta, fuera en el mismo país o en otro. Esta práctica – (...)-, fue lo que impulsó la expansión de las normas de propiedad intelectual y, sobre todo, los acuerdos internacionales en esta materia, como el famoso Convenio de Berna de 1886"[652].

El Convenio de Berna, firmado por 151 países, protege a las obras y a los derechos de los autores, permitiendo controlar quién, cómo y en qué condiciones se utilizan las obras objeto de protección. Establece tres principios básicos de protección: trato nacional, protección automática, e independencia; los cuales, en virtud del Acuerdo sobre los Aspectos de los Derechos de Propiedad Intelectual relacionados con el Comercio (ADPIC), también obligan a los Miembros de la Organización Mundial del Comercio (OMC).

Pero, como se mencionó anteriormente, el instrumento internacional de protección más antiguo es la Convención de Paris, de 1883, firmada por 96 países, y que dispone, entre otras cosas, el derecho de prioridad[653].

Conforme lo establecido en el artículo 2 del Convenio de Berna, la protección alcanza a las obras literarias y artísticas, lo cual comprende *"todas las producciones en el campo literario, científico y artístico, cualquiera que sea el modo o forma de expresión, tales como los libros, folletos y otros escritos; las conferencias, alocuciones, sermones y otras obras de la misma naturaleza las obras dramáticas o dramático-musicales; las obras coreográficas y las pantomimas; las composiciones musicales con o sin letra; las obras cinematográficas, a las cuales se asimilan las obras expresadas por procedimiento análogo a la cinematografía; las obras de dibujo, pintura,*

[652] Ibídem, pp. 49.

[653] Artículo 4. A. 1) del Convenio de Paris: "Quien hubiere depositado regularmente una solicitud de patente de invención, de modelo de utilidad, *de dibujo o modelo industrial, de marca de fábrica o de comercio, en alguno de los países de la Unión o su causahabiente, gozará, para efectuar el depósito en los otros países, de una derecho de prioridad, durante los plazos fijados más adelante en el presente".*

arquitectura, escultura, grabado, litografía; las obras fotográficas a las cuales se asimilan las expresadas por procedimiento análogo a la fotografía; las obras de artes aplicadas; las ilustraciones, mapas, planos, croquis y obras plásticas relativos a la geografía, a la topografía, a la arquitectura o a las ciencias."

El autor tiene derechos patrimoniales, los cuales pueden ser cedidos, y el derecho a reivindicar la paternidad de la obra, a oponerse a cualquier modificación de la misma, así como a cualquier atentado que le cause perjuicio a su honor o reputación[654]. Dichos derechos son mantenidos durante la vida del autor y hasta cincuenta años después de su muerte, y por lo menos hasta la extinción de los derechos patrimoniales. En el caso de las obras: (i) cinematográficas: el plazo expira a los 50 años después de que la obra haya sido accesible al público con el consentimiento del autor, o durante los cincuenta años siguientes a la realización de la obra; (ii) anónimas o seudónimas: el plazo de 50 años termina después de que haya sido accesible al público; (iii) fotográficas y artes aplicadas, la protección no puede ser menor a 25 años desde su realización[655].

Además, los autores tienen, entre otros, el derecho exclusivo de autorizar: (i) la tradición de sus obras[656]; (ii) la reproducción por cualquier procedimiento y bajo cualquier forma[657]; (iii) la radiodifusión de sus obras[658], así como la recitación pública y la transmisión pública por cualquier medio[659]; (iv) las adaptaciones, arreglos y otras transformaciones de sus obras[660]; y (v) la representación y ejecución pública[661].

Sin perjuicio, los países tienen la facultad de permitir la reproducción por la prensa o la transmisión al público de los artículos de actualidad de discusiones económicas, políticas o religiosas publicados en periódicos u en otros medios, debiendo indicar siempre la fuente. Asimismo, podrán ser reproducidas y accesibles al públicos, siempre que se justifique por el fin de la información[662].

Mas así como la tecnología y las telecomunicaciones impactan en múltiples áreas, lo mismo ocurre en la propiedad intelectual, generando grandes cambios que se han

[654] Artículo 6 BIS, 1), Convenio de Berna.
[655] Artículo 7 Convenio de Berna.
[656] Artículo 8, Convenio de Berna.
[657] Artículo 9, Convenio de Berna.
[658] Artículo 11Bis, Convenio de Berna.
[659] Artículo 11TER Convenio de Berna.
[660] Artículo 12, Convenio de Berna.
[661] Artículo 14, Convenio de Berna.
[662] Artículo 10, Convenio de Berna.

venido gestando desde hace muchos años y se han potenciado con el gran desarrollo de Internet y la computación.

Un antecedente directo se generó durante la Segunda Guerra Mundial, en tanto se invirtió mucho en el desarrollo de la tecnología. Uno de los principales ejemplos es la conocida Máquina de Turing, que se utilizó para desencriptar el código Enigma, lo cual permitió adelantarse a muchos de los movimientos de los alemanes contribuyendo en gran medida con el fin de la guerra. La máquina razonaba, seguía algoritmos, al tiempo que almacenaba, gestionaba e interpretaba los datos. De esta forma, se creó la posibilidad de almacenar y de gestionar los datos al mismo tiempo, permitiendo la transmisión y la reproducción de forma inmediata, sentando las bases fundamentales de la digitalización.[663]

En la sociedad de la información en que vivimos la información cobra cada vez mayor importancia, teniendo grandes impactos económicos y sociales, y planteando múltiples desafíos jurídicos.

Una muestra es la manifestada por Ian J. Lloyd, quien señala que cada vez más vemos empresas que son compradas no por su valor físico o por sus activos, sino por el valor de su propiedad intelectual, de su información. A modo de ejemplo, recuerda que en el 2012 Google pagó más de $12.5 billones por la tecnología de Motorola, y en gran parte por las 17.000 patentes de tecnología que tenían. Asimismo, también se ven casos y juicios millonarios entre las grandes empresas de tecnología, siendo el tema de gran actualidad e interés[664]. Asimismo, se ven muchos problemas con los video juegos y aquellos aspectos que pueden estar protegidos por marcas, así como derechos vinculados con los diseños del hardware, lo cual ha generado múltiples disputas, por ejemplo la guerra de las patentes por los smartphones entre Apple y Samsung[665]. También se presentan problemas con la jurisdicción. Al respecto, interesa mencionar el caso *HTC Europe Co Ltd v Apple Inc*, donde la Corte de Apelaciones sostuvo que una patente de Apple relacionada con la técnica usada en los iPhones y en los iPads para desbloquearlos era inválida, sosteniendo que la patente se mantenía válida solo en los Estados Unidos[666].

[663] Ibídem.,pp. 55.
[664] LLOYD, IAN, Information Technology Law, Oxford, 8th Edition, 2017, pp. 275.
[665] Ibídem, pp. 279.
[666] Ibídem, pp. 310.

Como enseña Lloyd, haciendo referencia a los orígenes de la PI pero que es una realidad que también se aplica a la actualidad, en 1707 los países relativamente pobres vieron pocos beneficios en las leyes de PI y ciertas ventajas en que no haya regulación. Los países más ricos, con más poder económico y político fueron quienes introdujeron las leyes de PI, pero para poder ser parte de la Organización Mundial de Comercio y acceder al Acuerdo General sobre Comercio y Aranceles, se tiene que aceptar también el Acuerdo sobre los Aspectos de los Derechos de Propiedad Intelectual (ADPIC), por lo que quienes firman el acuerdo reconocen los derechos de PI y tienen que proveer mecanismos para protegerlos, lo cual ha generado controversias, sobre todo en áreas relacionadas con la producción y la distribución de medicamentos, los cuales están protegidos por patentes. Asimismo, Lloyd reconoce que es cuestionable si el sistema de patentes afecta o no la innovación, y pone como ejemplo el caso de Elisha Gray y Alexander Bell. Personas diferentes pueden estar trabajando en proyectos similares de forma independiente, es un tema de chance y de método quien busca la protección primero, y es discutible si para la sociedad es bueno o no que alguien posea el monopolio en el desarrollo de tecnología o si es mejor que haya competidores para que haya más rápidos desarrollos[667]. Pero también es real que es necesario incentivar y proteger a quienes investigan e innovan.

Por otra parte, además de todas las implicancias vinculadas con las patentes, la protección de los derechos de autor es otro tema muy presente en la agenda digital, en tanto es esencial que las personas puedan acceder a los contenidos, a la información, a los efectos de seguir profundizando las creaciones e investigaciones; y al mismo tiempo, reconocer y garantizar los derechos a los autores y creadores como única forma de seguir impulsando el desarrollo y la innovación.

(IV.3) Protección Jurídica en España

La base es que el titular de la creación original es quien tiene el derecho a copiarla, así como a controlar si otros la copian, y la protección nace desde que la creación es expresada en algún medio.

La tecnología tiene gran impacto en este derecho, haciendo que el sistema se haya ido desarrollando a fin de ajustarse a las nuevas realidades y a las nuevas formas de expresión.

[667] Ibídem, p. 281.

En España los derechos de autor están protegida por la Constitución española (artículo 20,1,b), por la Ley de Propiedad Intelectual (LPI), por el Real Decreto Legislativo 1/1996, por sus normas reglamentarias, así como por el Código Civil y el Penal.

Vale señalar que parte de la doctrina considera que es un derecho de propiedad especial, y parte entiende que es un derecho fundamental adquiriendo dicho carácter como consecuencia de los instrumentos internacionales ratificados por el país. A los efectos del presente análisis lo consideraremos un derecho fundamental en base a lo dispuesto en el artículo 10.2 de la Constitución española: (Derechos de las personas) *"2. Las normas relativas a los derechos fundamentales y a las libertades que la Constitución reconoce se interpretarán de conformidad con la Declaración Universal de Derechos Humanos y los tratados y acuerdos internacionales sobre las mismas materias ratificados por España"*

La ley prevé que la PI de una obra literaria, artística o científica es del autor, por su creación[668], quien tiene la plena disposición y el derecho exclusivo a la explotación de la obra, estando integrada por derechos de carácter personal y patrimonial[669].

Se consideran objeto de protección *"todas las creaciones originales literarias, artísticas o científicas expresadas por cualquier medio o soporte, tangible o intangible, actualmente conocido o que se invente en el futuro, comprendiéndose entre ellas: a) Los libros, folletos, impresos, epistolarios, escritos, discursos y alocuciones, conferencias, informes forenses, explicaciones de cátedra y cualesquiera otras obras de la misma naturaleza. b) Las composiciones musicales, con o sin letra. c) Las obras dramáticas y dramático-musicales, las coreografías, las pantomimas y, en general, las obras teatrales. d) Las obras cinematográficas y cualesquiera otras obras audiovisuales. e) Las esculturas y las obras de pintura, dibujo, grabado, litografía y las historietas gráficas, tebeos o comics, así como sus ensayos o bocetos y las demás obras plásticas, sean o no aplicadas. f) Los proyectos, planos, maquetas y diseños de obras arquitectónicas y de ingeniería. g) Los gráficos, mapas y diseños relativos a la topografía, la geografía y, en general, a la ciencia. h) Las obras fotográficas y las expresadas por procedimiento análogo a la fotografía. i) Los programas de*

[668] Artículo 1 de la LPI.
[669] Artículo 2 de la LPI.

ordenador.[670]*".* Así como las obras derivadas, como ser: *"1.º Las traducciones y adaptaciones. 2.º Las revisiones, actualizaciones y anotaciones. 3.º Los compendios, resúmenes y extractos. 4.º Los arreglos musicales. 5.º Cualesquiera transformaciones de una obra literaria, artística o científica.*[671]*";* y las colecciones y bases de datos, entendiendo por tales *"las colecciones de obras, de datos, o de otros elementos independientes dispuestos de manera sistemática o metódica y accesibles individualmente por medios electrónicos o de otra forma"*[672].

Lo fundamental es que la obra debe ser creativa, original y debe estar expresada por cualquier medio. La originalidad refiere a la forma en que está expresada la idea, que no puede ser copiada de otro trabajo, no requiere que la idea en sí misma sea original.

La LPI expresamente excluye de la protección a las disposiciones legales o reglamentarias, así como sus proyectos, las resoluciones de órganos jurisdiccionales y los actos, acuerdos, deliberaciones y dictámenes de los organismos públicos, así como las traducciones oficiales de los antes mencionados[673].

Se considera que es "autor" la persona natural o jurídica que crea la obra literaria, artística o científica. La obra puede ser realizada de forma individual, en colaboración entre varios autores, colectiva[674], compuesta e independiente[675]. Además se deben contemplar los casos en que la obra es realizada por un empleado[676] , y la especificidad

[670] Artículo 10 de LPI
[671] Artículo 11 de LPI
[672] Artículo 12 de LPI
[673] Artículo 13 de LPI
[674] Artículo 8 de la LPI: *"Se considera obra colectiva la creada por la iniciativa y bajo la coordinación de una persona natural o jurídica que la edita y divulga bajo su nombre y está constituida por la reunión de aportaciones de diferentes autores cuya contribución personal se funde en una creación única y autónoma, para la cual haya sido concebida sin que sea posible atribuir separadamente a cualquiera de ellos un derecho sobre el conjunto de la obra realizada."*
[675] Artículo 9 de la LPI: *"1.Se considerará obra compuesta la obra nueva que incorpore una obra preexistente sin la colaboración del autor de esta última, sin perjuicio de los derechos que a éste correspondan y de su necesaria autorización. 2. La obra que constituya creación autónoma se considerará independiente, aunque se publique conjuntamente con otras."*
[676] Artículo 51 de la LPI: *"1. La transmisión al empresario de los derechos de explotación de la obra creada en virtud de una relación laboral se regirá por lo pactado en el contrato, debiendo éste realizarse por escrito. 2. A falta de pacto escrito, se presumirá que los derechos de explotación han sido cedidos en exclusiva y con el alcance necesario para el ejercicio de la actividad habitual del empresario en el momento de la entrega de la obra realizada en virtud de dicha relación laboral. 3. En ningún caso podrá el empresario utilizar la obra o disponer de ella para un sentido o fines diferentes de los que se derivan de lo establecido en los dos*

de cuando se trata de un programa de ordenador[677]. Si el autor es una persona natural, la protección será durante toda su vida y 70 años luego de su muerte, en caso de que el autor sea una persona jurídica, la protección será de 70 años desde el primero de enero del año siguiente al de la creación o divulgación de la creación.

Mas todo lo anterior presenta múltiples desafíos cuando se considera la Inteligencia Artificial. Basta con cuestionar si la obra creada por un robot está protegida, quién es el titular, y qué ocurre cuando infringe derechos de otros. Sobre este punto, interesa mencionar lo dispuesto por Patricia Fernández Céspedes, quien señala que LPI considera autor de una obra a la persona natural que la crea (artículo 5), con la excepción de las personas jurídicas, lo cual excluye de protección a las obras creadas por máquinas o por animales. En el caso de las obras realizadas por animales, recuerda el caso Naruto vs. Slater, en el que un mono se sacó una *selfie* con la cámara del fotógrafo David Slater. En dicho caso, una organización de protección de animales reclamó la autoría del mono sobre la foto, dado que en Estados Unidos tiene el derecho de autor quien saca la foto y no quien es el dueño de la cámara. Sin perjuicio, un Tribunal en San Francisco resolvió otorgar los derechos al fotógrafo dado que dichos derechos no podían reconocerse a un animal. En lo que respecta a las máquinas, aún no hay posición alguna al respecto. Vale destacar que tradicionalmente las personas programaban las máquinas, pero con el desarrollo de la inteligencia artificial y con el hecho de que las máquinas tienen la posibilidad de aprender automáticamente, tomando

---

apartados anteriores. 4. Las demás disposiciones de esta Ley serán, en lo pertinente, de aplicación a estas transmisiones, siempre que así se derive de la finalidad y objeto del contrato. 5. La titularidad de los derechos sobre un programa de ordenador creado por un trabajador asalariado en el ejercicio de sus funciones o siguiendo las instrucciones de su empresario se regirá por lo previsto en el apartado 4 del artículo 97 de esta Ley."

[677] Artículo 97 de la LPI*: "Artículo 97. Titularidad de los derechos. 1. Será considerado autor del programa de ordenador la persona o grupo de personas naturales que lo hayan creado, o la persona jurídica que sea contemplada como titular de los derechos de autor en los casos expresamente previstos por esta Ley. 2. Cuando se trate de una obra colectiva tendrá la consideración de autor, salvo pacto en contrario, la persona natural o jurídica que la edite y divulgue bajo su nombre. 3. Los derechos de autor sobre un programa de ordenador que sea resultado unitario de la colaboración entre varios autores serán propiedad común y corresponderán a todos éstos en la proporción que determinen. 4. Cuando un trabajador asalariado cree un programa de ordenador, en el ejercicio de las funciones que le han sido confiadas o siguiendo las instrucciones de su empresario, la titularidad de los derechos de explotación correspondientes al programa de ordenador así creado, tanto el programa fuente como el programa objeto, corresponderán, exclusivamente, al empresario, salvo pacto en contrario. 5. La protección se concederá a todas las personas naturales y jurídicas que cumplan los requisitos establecidos en esta Ley para la protección de los derechos de autor".*

decisiones propias, para lo cual no necesariamente fueron previamente configuradas, la responsabilidad pasa a ser menos manifiesta[678].

Es interesante mencionar que el Parlamento Europeo aprobó el Texto (P8_TA(2017)0051) "Normas de Derecho civil sobre robótica"[679], donde señaló que si bien no hay disposiciones jurídicas que se apliquen específicamente a la robótica, las doctrinas y los regímenes jurídicos actuales pueden aplicarse, aunque algunos aspectos requieran especial consideración. Se hace énfasis en un enfoque horizontal y de neutralidad tecnológica para la propiedad intelectual. Asimismo, *"observa que el desarrollo de la tecnología robótica requerirá una mayor comprensión de las bases comunes necesarias para la actividad conjunta humano-robótica, que debe basarse en dos relaciones de interdependencia básicas, a saber, la previsibilidad y la direccionalidad; señala que estas dos relaciones de interdependencia son fundamentales para determinar qué información debe ser compartida entre seres humanos y robots, y cómo puede conseguirse una base común entre seres humanos y robots que permita una acción conjunta humano-robótica eficaz[680]"*. Finalmente, señala que *"Cabría garantizar la interoperabilidad de los robots autónomos conectados a la red autónoma que interactúan entre sí. El acceso al código fuente, a los datos de entrada y a los detalles de construcción debería estar disponible cuando fuera necesario, para investigar tanto los accidentes como los daños causados por «robots inteligentes», así como para velar por su funcionamiento, disponibilidad, fiabilidad, seguridad y protección continuados".*

Vale mencionar que la Comisión Europea presentó en abril de 2018 una seria de medidas para poner a la inteligencia Artificial al servicios de los ciudadanos europeos e impulsar la competitividad en Europa. En dicha oportunidad propuso, entre otras cosas: (i) reforzar la inversión pública y privada en Inteligencia Artificial, en tanto parte de la base de que los datos son la materia prima de la mayoría de las tecnologías; (ii) anticipar los cambios socioeconómicos: siendo fundamental la capacitación digital, las competencias en los ámbitos de ciencia, tecnología, ingeniería y matemáticas (CTIM o

[678] FERNÁNDEZ, PATRICIA, "El hombre contra la máquina, ¿puede un robot ostentar derechos de propiedad intelectual?. URL: https://www.bamboo.legal/inteligencia-artificial-derechos-de-autor/ Consultado el 20 de enero de 2020.

[679] Parlamento Europeo: Normas de Derecho Civil sobre robótica. URL: https://www.europarl.europa.eu/doceo/document/TA-8-2017-0051_ES.pdf?redirect Consultado el 20 de enero de 2020.

[680] https://www.europarl.europa.eu/doceo/document/TA-8-2017-0051_ES.pdf?redirect Consultado el 20 de enero de 2020.

STEM), el espíritu empresarial y la creatividad; y (iii) garantizar un marco ético y jurídico adecuado: principalmente en lo que respecta a la responsabilidad y a la toma decisiones potencialmente sesgada.[681]

Además, es de mención la Propuesta de Resolución del Parlamento Europeo sobre una política industrial global europea en materia de inteligencia artificial y robótica (2018/2088(INI)), donde se subraya la necesidad de supervisar la pertinencia y la eficiencia de las normas sobre derechos de propiedad intelectual en relación a la inteligencia artificial.[682]

Siguiendo con la LPI, los programas de ordenador se rigen por los preceptos del Título VII, entendiendo por tales *"toda secuencia de instrucciones o indicaciones destinadas a ser utilizadas, directa o indirectamente, en un sistema informático para realizar una función o una tarea o para obtener un resultado determinado, cualquiera que fuere su forma de expresión y fijación.[683]".* Comprende además la documentación preparatoria, la técnica y los manuales de uso. Se considera que son autores del programa la persona o el grupo de personas naturales que lo hayan creado, o la persona jurídica que sea contemplada como titular de los derechos de autor[684].

Se prevé la protección "sui generis" de las bases de datos, entendiendo por tales *"las colecciones de obras, de datos, o de otros elementos independientes dispuestos de manera sistemática o metódica y accesibles individualmente por medios electrónicos o de otra forma*[685]". La protección alcanza a "la inversión sustancial, evaluada cualitativa o cuantitativamente, que realiza su fabricante ya sea de medios financieros, empleo de tiempo, esfuerzo, energía u otros de similar naturaleza, para la obtención, verificación o presentación de su contenido[686]". Por este derecho, el fabricante de una base de datos[687],

---

[681] Comunicado de prensa, 24 de abril de 2018, "Inteligencia artificial: la Comisión presenta un enfoque europeo para impulsar la inversión y establecer directrices éticas". URL: https://ec.europa.eu/commission/presscorner/detail/es/IP_18_3362 _ Consultado el 20 de enero de 2020.

[682] Parlamento Europeo, sobre una política industrial global europea en materia de inteligencia artificial y robótica (2018/2088(INI)). URL: https://www.europarl.europa.eu/doceo/document/A-8-2019-0019_ES.html Consultado el 20 de enero de 2020.

[683] Artículo 95 de la LPI.

[684] Artículo 97 de la LPI.

[685] Artículo 12.2 de la LPI.

[686] Artículo 133 de la LPI.

[687] Entendiendo por tal a la "*persona natural o jurídica que toma la iniciativa y asume el riesgo de efectuar las inversiones sustanciales orientadas a la obtención, verificación o presentación de su contenido".* (Artículo 133.3.a) LPI).

"puede prohibir la extracción y/o reutilización de la totalidad o de una parte sustancial del contenido de ésta, evaluada cualitativa o cuantitativamente, siempre que la obtención, la verificación o la presentación de dicho contenido representen una inversión sustancial desde el punto de vista cuantitativo o cualitativo. Este derecho podrá transferirse, cederse o darse en licencia contractual.[688] "

Como enseña Susana Checa Prieto, *"La protección de derechos de autor le corresponderá a la base de datos creada, como obra intelectual, y tendrá las mismas características que el resto de obras protegibles, mientras que el derecho sui generis protege la indexación de la obra, impidiendo legalmente que alguien pueda descargarse la totalidad o una parte sustancial del contenido de la base de datos mediante el motor de búsqueda de ésta y luego pueda crear otra base de datos con una interfaz distinta y explotarla. Es decir, si yo contrato una base de datos tengo derecho a descargarme y utilizar todo su contenido, pero no tendrá derecho a comercializarlo posteriormente. Además, en las bases de datos existe otro derecho, que es el de los autores de las obras contenidas en la propia base de datos, si es que los tienen.*[689] "

(IV.4) Protección jurídica en Uruguay.

La Propiedad intelectual en Uruguay comprende los derechos de autor y la propiedad industrial.

Los derechos de autor están regulados por las Ley 9.739, con diversas modificaciones introducidas por las leyes 17.616, 17.805. 18.046 y 19.149, y por sus decretos reglamentarios. Además, entre otras normas, por lo establecido en la Declaración Universal de Derechos Humanos de 1948, en el Convenio de Berna, en la Convención Internacional sobre Protección de artistas, intérpretes o ejecutantes, Productores de Fonogramas y Organismos de Radiodifusión de 1961, el Convenio para la Protección de los Productores de fonogramas contra la Reproducción no autorizada de sus Fonogramas de 1971, y el AADPIC, Anexo 1C.

La ley protege: (i) el derecho moral del autor de toda creación literaria, científica o artística y le reconoce derecho de dominio sobre las producciones de su pensamiento, ciencia o arte; (ii) los derechos de los artistas, intérpretes y ejecutantes, productores de

[688] Artículo 133.1, párrafo segundo, de la LPI.
[689] CHECA PRIETO Susana, en Nota Técnica 3, "Los Derechos de Autor", Máster de Acceso a la Abogacía, Derecho Informático y Nuevas Tecnologías, Universidad de Nebrija. Año 2019.

fonogramas y organismos de radiodifusión[690]. Comprende las expresiones, pero no las ideas, procedimientos, métodos de operación o conceptos matemáticos en sí[691].

En esta línea, el derecho de propiedad intelectual comprende la facultad del autor de enajenar, reproducir[692], distribuir[693], publicar[694], traducir[695], adaptar, transformar, comunicar[696] o poner a disposición del público[697] las mismas, en cualquier forma o procedimiento.

La ley expresamente manifiesta lo que la producción intelectual, científica o artística comprende. Si bien parecería una enumeración taxativa, al cierre se hace referencia a *"toda producción del dominio de la inteligencia"*[698] lo cual permite extender mucho la aplicación, comprendiendo trabajos de autoría original y no alcanzando a las ideas.

Vale destacar que esta interpretación fue la sostenida por el Poder Ejecutivo, Ministerio de Educación y Cultura, en el mensaje de Proyecto de Ley sobre el Derecho

---

[690] Artículo 1 de la Ley 9.739 actualizada.
[691] Artículo 5 de la Ley 9.739.
[692] Comprende la fijación de la obra o producción, en cualquier forma o por cualquier procedimiento, incluyendo la obtención de copias, su almacenamiento electrónico, que posibilite su percepción o comunicación.(Artículo 2, inc. 2, de la Ley 9739).
[693] Comprende la puesta a disposición del público del original o una o más copias de la obra o producción, mediante su venta, permuta u otra forma de transmisión de la propiedad, arrendamiento, préstamo, importación, exportación o cualquier otra forma conocida o por conocerse, que implique la explotación de las mismas. (Artículo 2, inc. 3, de la Ley 9739).
[694] Comprende el uso de la prensa, de la litografía, del polígrafo y otros procedimientos similares; la transcripción de improvisaciones, discursos, lecturas, etcétera, aunque sean efectuados en público, y asimismo la recitación en público, mediante la estenografía, dactilografía y otros medios. (Artículo 2, inc. 4, de la Ley 9739).
[695] Comprende la traducción de lenguas y de dialectos. (Artículo 2, inc. 5, de la Ley 9739).
[696] Comprende la representación y la ejecución pública de las obras, por cualquier medio o procedimiento, sea con la participación directa de intérpretes o ejecutantes, o recibidos o generados por instrumentos o procesos mecánicos, ópticos o electrónicos, o a partir de una grabación sonora o audiovisual, u otra fuente; la proyección o exhibición pública de las obras cinematográficas y demás obras audiovisuales; la transmisión o retransmisión de cualesquiera obras por radiodifusión u otro medio de comunicación inalámbrico, o por hilo, cable, fibra óptica u otro procedimiento análogo que sirva para la difusión a distancia de los signos, las palabras, los sonidos o las imágenes, sea o no mediante suscripción o pago; la puesta a disposición, en lugar accesible al público y mediante cualquier instrumento idóneo, de la obra transmitida o retransmitida por radio o televisión; la exposición pública de las obras de arte o sus reproducciones. (Artículo 2, inc. 6, de la Ley 9739).
[697] Comprende, todo acto mediante el cual la obra se pone al alcance del público, por cualquier medio o procedimiento, incluyendo la puesta a disposición del público de las obras, de tal forma que los miembros del público puedan acceder a estas obras desde el lugar y en el momento que cada uno de ellos elija. (Artículo 2, inc. 7, de la Ley 9739).
[698] Artículo 5 de la Ley 9739.

de autor y Derechos Afines, remitido en Mayo de 2000: *"…cualquier enumeración que se haga de las creaciones tuteladas tiene un carácter simplemente ejemplificativo.*

Así aparece, por lo demás, en la Convención Universal (art. 1) y en el Convenio de Berna (art. 2), al preceder la indicación de las obras protegidas con la expresión "tales como", lo que también se ha incorporado a la mayoría de las legislaciones nacionales con algunos de estos vocablos: "en particular" (Alemania, Italia), "principalmente" (Brasil), "especialmente" (Chile, Francia, Venezuela), "tales como" (Colombia, Costa Rica), "incluyendo, pero no limitados" (República Dominicana, art. 2), "fundamentalmente" (Cuba, art. 7), "todas las demás que por analogía ..." (v. gr.: El Salvador, México), "entre otras" (Decisión Andina 351), u otras de similar sentido, y que ya figuraba en la Ley 9.739 (art. 5°), al proteger "y, en fin, toda producción del dominio de la inteligencia". (…)

Coadyuva asimismo al carácter meramente ejemplificativo del catálogo, la frase final, inspirada en la Convención de Washington y acogida por recientes legislaciones (v.gr.: Panamá, Venezuela) y en varios proyectos legislativos (v.gr.:Paraguay, Perú), según la cual queda protegida "en general, toda producción del intelecto en el dominio literario o artístico, que tenga características de originalidad y sea susceptible de ser divulgada o reproducida por cualquier medio o procedimiento, conocido o por conocer".

En cualquier caso, la enumeración ejemplificativa del artículo 5° sigue en lo esencial la redacción del artículo 2,1 del Convenio de Berna, con la particularidad de sustituir la mención de las obras cinematográficas u otras obtenidas por un procedimiento análogo, por la más omnicomprensiva de "obras audiovisuales", como se explicará en su oportunidad; la incorporación expresa de los programas de ordenador, conforme al Acuerdo ADPIC y la tendencia en el Derecho Comparado; y la mención explícita de las bases de datos (también en concordancia con el Acuerdo ADPIC y las modernas legislaciones), siempre que, como en las demás compilaciones, "la selección o disposición de las materias constituyan creaciones intelectuales".[699] *"*

[699] Mensaje del Proyecto de ley sobre el Derecho de Autor y Derechos afines, Ministerio de Educación y Cultura de Uruguay. Mayo 2000. URL: http://archivo.presidencia.gub.uy/noticias/archivo/2000/mayo/2000052300.htm Consultado el 20 de enero de 2020.

En esta línea, entre las producciones expresamente se mencionan las siguientes: (i) composiciones musicales con o sin palabras impresas o en discos, cilindros, alambres o películas, siguiendo cualquier procedimiento de impresión, grabación o perforación, o cualquier otro medio de reproducción o ejecución: cartas, atlas y mapas geográficos; escritos de toda naturaleza. (ii) Folletos. (iii) Fotografías. (iv) Ilustraciones. (v) Libros. (vi) Consultas profesionales y escritos forenses. (vii) Obras teatrales, de cualquier naturaleza o extensión, con o sin música. (viii) Obras plásticas relativas a la ciencia o a la enseñanza. (ix) Obras audiovisuales, incluidas las cinematográficas, realizadas y expresadas por cualquier medio o procedimiento. (x) Obras de dibujo y trabajos manuales. (xi) Documentos u obras científicas y técnicas. (xii) Obras de arquitectura. (xiii) Obras de pintura. (xiv) Obras de escultura. (xv) Fórmulas de las ciencias exactas, físicas o naturales, siempre que no estuvieren amparadas por leyes especiales. (xvi) Obras radiodifundidas y televisadas. (xvii) Textos y aparatos de enseñanza.(xviii) Grabados. (xix)Litografía. (xx) Obras coreográficas cuyo arreglo o disposición escénica "*mise en scene*" esté determinada en forma escrita o por otro procedimiento. (xxi) Títulos originales de obras literarias, teatrales o musicales, cuando los mismos constituyen una creación. (xxii) Pantomimas. (xxiii) Pseudónimos literarios. (xxiv) Planos u otras producciones gráficas o estratigráficas, cualquiera sea el método de impresión. (xxv) Modelos o creaciones que tengan un valor artístico en materia de vestuario, mobiliario, decorado, ornamentación, tocado, galas u objetos preciosos, siempre que no estuvieren amparados por la legislación vigente sobre propiedad industrial.

Finalmente, se hace mención:

- a los programas de ordenador, sean programas fuente o programas objeto;

- a las bases de datos, entendiendo por tales a las compilaciones de datos o de otros materiales, en cualquier forma, que por razones de la selección o disposición de sus contenidos constituyan creaciones de carácter intelectual. Expresamente se aclara que no comprende a los datos en sí, sino que refiere a la expresión de las ideas, de la información y de los algoritmos, siempre que sean presentados de forma original y apropiada para ser utilizado por un dispositivo de procesamiento de información o de control automático

- a toda producción del dominio de la inteligencia.

Resulta realmente interesante esta última expresión "*toda producción del dominio de la inteligencia"*. Como surge de la exposición de motivos, la expresión adrede es muy amplia, pudiendo comprender un sinfín de creaciones originales, además podría interpretarse que no se limita quién podría ser el titular de esos derechos.

En relación a este último punto, vale destacar que el artículo 4 de la Ley 9739 dispone que la protección legal será acordada en todos los casos, cualquiera sea la naturaleza o la procedencia de la obra o la nacionalidad del autor, sin distinción. Además, el artículo 6 de la Ley 9739 dispone que el goce y ejercicio del derecho no está subordinado a ninguna formalidad o registro, y es independiente de la existencia de protección en el país de origen de la obra. Además, si bien el artículo 7 de la misma Ley dispone que son titulares del derecho: (i) el autor de la obra y sus sucesores, (ii) los colaboradores, (iii) los adquirentes a cualquier título, (iv) los traductores y los que actúen en obras ya existentes (refundiéndolas, adaptándolas, modificándolas, etc.), (v) el artista intérprete o ejecutante, (vi) el Estado; las referencias nuevamente son muy amplias, no disponiendo limitación de clase alguna respecto a quién puede ser el autor o el titular de la obra. No obstante, se debe advertir que únicamente pueden ser titulares de derechos morales las personas físicas.

En definitiva, del texto de la norma podría válidamente considerarse que la protección abarca a toda producción del dominio de la inteligencia, cualquiera sea la naturaleza o procedencia de la obra.

Sin perjuicio, vale destacar que Beatriz Bugallo señala que el autor es la persona física que lleva a cabo la creación, que en caso de persona jurídica, la misma puede ser titular de derecho, pero no el autor, siendo titular originario en caso de obras colectivas[700].

Respecto a los Derechos, Bugallo destaca los derechos morales: paternidad, integridad, modificación, retracto; y los derechos de explotación: de contenido patrimonial, que pueden embargarse y tienen un plazo determinado de duración[701].

---

[700] BUGALLO, BEATRIZ, "Manual de Propiedad Intelectual". URL: https://drive.google.com/file/d/1rE92X76p2GHXEHoEFcF_6mmQTpO3OY1e/view Consultado el 20 de enero de 2020. pp. 169.

[701] Ibídem, p. 170.

El derecho está limitado en el tiempo, salvo cuando el titular es el Estado, o cualquier organismo público, que será a perpetuidad. El autor conserva su derecho durante toda su vida, y los herederos o legatarios por 40 años desde el fallecimiento del autor. Si la obra no fue publicada dentro de los 10 años desde el fallecimiento, caerá en dominio público[702]. En el caso obras anónimas y seudónimas, el plazo de protección es de 50 años desde que está accesible al público[703]. Las obras en colaboración constituyen copropiedad indivisa, y salvo pacto en contrario, da a los coautores los mismos derechos[704].

Los derechos de autor, de carácter patrimonial, son transmisibles, debiendo constar por escrito, pero para que sean oponible deben estar registrados en el Registro de Derechos de Autor. Sin perjuicio, el autor tiene el derecho a exigir la mención de su nombre o pseudónimo y el título de la obra, a vigilar las publicaciones, representaciones, ejecuciones, reproducciones o traducciones, así como a oponerse a que el título, texto, composición, etc., sean suprimidos, supuestos, alterados, etc; así como a corregir o modificar la obra enajenada siempre que no altere su carácter o finalidad y no perjudique el derecho de terceros adquirentes de buena fe[705]. Cuando una obra pase al dominio público, cualquier persona podrá explotarla[706].

En definitiva, como enseña Beatriz Bugallo*: "La propiedad literaria y artística o derechos de autor y derechos conexos comprende la protección de los autores de un muy variado elenco de obras, pues si son obras protegidas todas las creaciones del ingenio humano. (...) incluye también la protección del software, que está amparado en la legislación uruguaya por el régimen de los derechos de autor*". Así, Bugallo señala que este derecho tiene una doble consideración, por un lado normas que regulan bienes incorporales en particular, y por otro normas que regulan la competencia[707].

En relación al uso de artículos en periódicos, revistas u otros medios de comunicación social, salvo pacto en contrario, la autorización otorgada por el autor solo confiere al editor o propietario de la publicación, el derecho de utilizarlo por una vez, quedando a salvo los demás derechos patrimoniales del cedente o licenciatario. La

[702] Artículo 14 de la ley 9739.
[703] Artículo 17 de la 9739.
[704] Artículo 26 de la Ley 9739.
[705] Artículo 12 de la ley 9739.
[706] Artículo 42 de la ley 9739.
[707] BUGALLO, BEATRIZ, obra citada. pp. 169.

utilización del artículo en medios distintos o con fines distintos debe contar con la autorización del autor[708]. Lo mismo se aplica para dibujos, chistes, gráficos, caricaturas, fotografías y demás obras susceptibles de ser publicadas en periódicos, revistas u otros medios de comunicación social[709].

(IV.5) Desafíos de los Derechos de Autor en la era digital

Respecto a la protección del software. Si bien, a diferencia de lo que ocurre con las patentes, no cabe duda de que el software tiene protección por los derechos de autor, hay vacilaciones respecto al alcance, para lo cual es fundamental atender si se tuvo acceso al trabajo original y si el resultado es sustancialmente similar[710].

Por otra parte, entre los grandes desafíos que enfrentan los derechos de autor, además de los comentados en relación a la inteligencia artificial y a la robótica, se destacan principalmente los vinculados al gran desarrollo de Internet y al intercambio constante de información entre diversas plataformas y sitios web de forma universal; en tanto permite que se hagan billones de copias, de forma inmediata, constante y que se distribuyan alrededor del mundo, sin prácticamente limitación o control alguno.

En este sentido, como se señala en la Propuesta de Directiva Del Parlamento Europeo y del Consejo sobre los derechos de autor en el Mercado Único Digital, del 14.9.2016 COM(2016) 593 final, es necesario adaptar las normativas referentes a la materia en tanto *"La evolución de las tecnologías digitales ha transformado la manera en que se crean, producen, distribuyen y explotan las obras y otras prestaciones protegidas. Han surgido nuevos usos, así como nuevos intervinientes y nuevos modelos de negocio. En el entorno digital, se han intensificado también los usos transfronterizos, y han surgido nuevas oportunidades para que los consumidores puedan acceder a contenidos protegidos por derechos de autor."*

Internet tiene un rol fundamental, en tanto facilita el acceso y la distribución, pero al mismo tiempo genera dificultades para conceder licencias, así como para controlar sus derechos, lo cual limita los incentivos para innovar y crear.

[708] Artículo 22 de la Ley 9739.
[709] Artículo 24 de la Ley 9739.
[710] LLOYD, IAN, obra citada, pp. 279.

Se explicita la necesidad de que haya coherencia en la regulación, y se prevé la necesidad de crear un marco moderno de los derechos de autor, tomando como base, entre otras, las siguientes Directivas:

- 96/9/CE, sobre la protección jurídica de las bases de datos.
- 2001/29/CE8, relativa a la armonización de determinados aspectos de los derechos de autor y derechos afines a los derechos de autor en la sociedad de la información.
- 2006/115/CE9, sobre derechos de alquiler y préstamo y otros derechos afines a los derechos de autor en el ámbito de la propiedad intelectual.
- 2009/24/CE10, sobre la protección jurídica de programas de ordenador.
- 2012/28/UE11, sobre ciertos usos autorizados de las obras huérfanas.
- 2014/26/UE12, relativa a la gestión colectiva de los derechos de autor y derechos afines y a la concesión de licencias multiterritoriales de derechos sobre obras musicales para su utilización en línea en el mercado interior.
- 2010/13/UE, sobre la coordinación de determinadas disposiciones legales, reglamentarias y administrativas de los Estados miembros relativas a la prestación de servicios de comunicación audiovisual.

Entre los principales problemas que se identificaron para asegurar los derechos de autor y las prácticas conexas, se destacaron la existencia de problemas con la aplicación de determinadas excepciones, la ausencia de efectos transfronterizos y dificultades en la utilización de contenidos protegidos por derechos de autor, como ser en los ámbitos de la investigación, la educación y la conservación del patrimonio cultural.

A modo de ejemplo, se señala específicamente la minería de textos y datos, la cual permite a los investigadores tratar grandes cantidades de datos impulsando la innovación. Sin perjuicio, se identifica que hay inseguridades en tanto se pueden llegar a vulnerar derechos de autor, así como el derecho sui generis de las bases de datos, en casos de reproducción de obras o de extracción de contenidos[711], siendo necesario dar

[711] Propuesta de Directiva del Parlamento Europeo y del Consejo sobre los derechos de autor en el mercado único digital, COM/2016/0593 final – 2016/0280 (COD). Exposición de motivos (8).

seguridad en estos puntos para que la Unión Europea se pueda seguir desarrollando en materia de investigación[712].

Asimismo, se señala que los proveedores de servicios de la sociedad de la información almacenan y facilitan el acceso público a obras dispuestas online por diversos usuarios, lo cual puede afectar derechos de autor[713]; y se hace énfasis en la importancia de trabajar con los proveedores de servicios que almacenan y facilitan el acceso a dichas obras para el funcionamiento de herramientas tecnológicas como son las de reconocimiento de contenido[714].

Considerando lo antes dicho, se remitió una propuesta de Directiva del Parlamento Europeo y del Consejo sobre los derechos de autor en el mercado único digital el 14 de setiembre de 2016, la cual, luego de diversas vacilaciones, fue aprobada Directiva (UE) 2019/790 el 26 de marzo de 2019, publicada el 17 de mayo de 2019 en el Boletín Oficial Europeo, dando dos años a los países miembros para su implementación.

Como surge de la exposición de motivos, al analizar el impacto de la propuesta, se generaron principalmente tres títulos. Uno relacionado con garantizar un amplio acceso a los contenidos, adaptando las excepciones y limitaciones al entorno digital y transfronterizo. Otro, vinculado con mejorar las prácticas de concesión de licencias y garantizar un mayor acceso a los contenidos; y otro buscando que el mercado para los derechos de autor funcione adecuadamente.

En este sentido, como se señala en el artículo 1 de la Directiva (UE) 2019/790, el objeto es armonizar el derecho de la Unión aplicable a los derechos de autor y derechos afines, en vista de los usos digitales y transfronterizos de los contenidos protegidos; así como establecer normas relacionadas con las excepciones y limitaciones, facilitar las licencias y, en definitiva, garantizar el correcto funcionamiento del mercado de explotación de obras y otras prestaciones.

---

[712] Propuesta de Directiva del Parlamento Europeo y del Consejo sobre los derechos de autor en el mercado único digital, COM/2016/0593 final – 2016/0280 (COD). Exposición de motivos (9).

[713] Propuesta de Directiva del Parlamento Europeo y del Consejo sobre los derechos de autor en el mercado único digital, COM/2016/0593 final – 2016/0280 (COD). Exposición de motivos (38).

[714] Propuesta de Directiva del Parlamento Europeo y del Consejo sobre los derechos de autor en el mercado único digital, COM/2016/0593 final – 2016/0280 (COD). Exposición de motivos (39).

Respecto a las medidas para adaptar las excepciones y limitaciones al entorno digital y transfronterizo:

El artículo 3 establece la excepción referente a las reproducciones y extracciones realizadas por organismos de investigación e instituciones responsables del patrimonio cultural con el fin de realizar, con fines de investigación científica, minería de textos y datos de obras u otras prestaciones a las que tengan acceso lícito. Asimismo, se prevé la posibilidad de almacenarlas con un nivel adecuado de seguridad y conservarlas para fines de investigación científica; y el derecho de los titulares de derechos de aplicar medidas que sean necesarias para garantizar la seguridad e integridad de las redes y bases de datos.

El artículo 5 prevé la utilización de obras y otras prestaciones en actividades pedagógicas digitales y transfronterizas, previendo una excepción o limitación para fines de enseñanza a efectos de ilustración con fines educativos no comerciales, siempre que el uso sea bajo la responsabilidad de un centro de enseñanza, ya sea en sus locales o en otros lugares, o a través de una red electrónica de los alumnos o estudiantes y el personal docente del centro, y que esté acompañado de la fuente, con inclusión del nombre del autor.

El artículo 6 prevé la realización de copias para la conservación del patrimonio cultural.

En relación a las medidas para mejorar las prácticas de concesión de licencias y garantizar un mayor acceso a los contenidos, se prevé:

por un lado, lo referente a obras y prestaciones fuera del circuito comercial, específicamente: (i) el uso de obras que están fuera del circuito comercial por parte de las instituciones de patrimonio cultural[715], (ii) el uso transfronterizo[716], (iii) las medidas de publicidad sobre la información relativa a las licencias, a los territorios cubiertos y los usos, a fin de que sean accesibles permanentemente, con facilidad y de manera efectiva[717], y (iv) el diálogo entre las organizaciones de usuarios y titulares de derechos representativas, así como con otras organizaciones pertinentes, para fomentar facilitar el

[715] Artículo 8 de la Directiva (UE) 2019/790
[716] Artículo 9 de la Directiva (UE) 2019/790
[717] Artículo 10 de la Directiva (UE) 2019/790

uso de los mecanismos de concesión y por la eficacia de las salvaguardias para los titulares de los derechos[718].

Por otro lado, las medidas para facilitar la concesión de licencias colectivas, estableciendo la posibilidad de ampliar el efecto del acuerdo, en lo que refiere al territorio[719].

Asimismo, se prevé el acceso y disposición de obras audiovisuales en plataformas de video a la carta, disponiendo mecanismos de negociación[720].

Posteriormente, en relación a las obras de arte visual de dominio público, señalan que una vez que haya expirado el plazo de protección de una obra de arte visual, la reproducción no estará sujeta a derechos de autor, a menos que el material resultante sea original y sea una creación intelectual del autor.

Finalmente, para garantizar el funcionamiento del mercado de derechos de autor, se disponen diversas medidas, entre ellas:

se protegen las publicaciones de prensa en lo relativo a los usos en línea, reconociendo, por un plazo de dos años, a las editoriales de publicaciones de prensa, los derechos de reproducción, así como de autorizar o prohibir la puesta a disposición del público de obras protegidas, para el uso en línea de sus publicaciones de prensa por parte de prestadores de servicios de la sociedad de la información[721], lo cual no se aplicará al uso privado o no comercial por parte de los usuarios individuales, ni a los actos de hiperenlace, ni a palabras sueltas o de extractos muy breves.

Se señala que cuando un autor haya cedido o concedido una licencia de un derecho a una editorial, tal cesión o licencia permite que la editorial tenga derecho a una parte de la compensación por el uso de la obra que se haya efectuado en el marco de dicha excepción o limitación del derecho cedido u objeto de licencia[722].

Se prevé el uso de contenidos protegidos por parte de proveedores de servicios para compartir contenidos en línea. Se señala que los prestadores de servicios, requerirán autorización de los titulares, para compartir contenidos o para poner a

[718] Artículo 11 de la Directiva (UE) 2019/790
[719] Artículo 12 de la Directiva (UE) 2019/790
[720] Artículo 13 de la Directiva (UE) 2019/790
[721] Artículo 15 de la Directiva (UE) 2019/790
[722] Artículo 16 de la Directiva (UE) 2019/790

disposición del público el acceso a obras protegidas por derechos de autor u otras prestaciones protegidas que hayan sido cargadas por sus usuarios[723].

Adicionalmente, se prevé la remuneración equitativa de los autores y artistas intérpretes o ejecutantes en los contratos de explotación. En este sentido, se establece: (i) el principio de remuneración adecuada y proporcionada[724]; (ii) la obligación de transparencia, que se asegure que *"l*os *autores y los artistas intérpretes o ejecutantes reciban periódicamente, y por lo menos una vez al año, teniendo en cuenta las características específicas de cada sector, información actualizada, pertinente y exhaustiva sobre la explotación de sus obras e interpretaciones o ejecuciones por las partes a las que hayan concedido licencias o cedido sus derechos, o de los derechohabientes de estos, especialmente en lo que se refiere a los modos de explotación, la totalidad de los ingresos generados y la remuneración correspondiente.[725]";* (iii) mecanismos de adaptación de contratos, a fin de que se vele por que los autores y los artistas intérpretes o ejecutantes o sus representantes tengan derecho a solicitar una remuneración adicional, adecuada y equitativa para la explotación de sus derechos, en caso de que la remuneración inicialmente pactada sea desproporcionadamente baja en comparación con las ingresos y beneficios subsiguientes derivados de la explotación de las obras o interpretaciones[726]. (iv) Se disponen la adopción de mecanismos de resolución de litigios relativos a la obligación de transparencia y al mecanismo de adaptación de contratos, previendo procedimientos alternativos de resolución de litigios de carácter voluntario[727]. (v) El derecho de revocación, en caso de que la obra o prestación protegida cedida o licenciada ya no se esté explotando[728].

Estas medidas, principalmente las relativas a la posibilidad de cobrar a los servicios online por usar el contenido periodístico, así como la creación de un mercado de licencias y de responsabilidad, han sido muy criticado por diversas organizaciones, sobre todo por entender que puede afectar derechos humanos como es el derecho al acceso de la información y la libertad de expresión.

[723] Artículo 17 de la Directiva (UE) 2019/790
[724] Artículo 18 de la Directiva (UE) 2019/790
[725] Artículo 19 de la Directiva (UE) 2019/790
[726] Artículo 20 de la Directiva (UE) 2019/790
[727] Artículo 21 de la Directiva (UE) 2019/790
[728] Artículo 22 de la Directiva (UE) 2019/790

Al respecto, interesa recordar jurisprudencia del TJUE, como ser *Productores de Música de España (Primusicae) v. Telefónica de España, S.A., asunto C-275/06, y Johan Deckmyn y Vrijheidsfonds VZW, asunto C-201/13*, donde destaca la importancia de los justos equilibrios entre los derechos fundamentales, respetar su finalidad y considerar la proporcionalidad[729].

Por otra parte, como señala Sebastián Cabello[730], la prensa tiene problemas de sostenibilidad, y haciendo mención al Instituto Reuters en su Digital News Report 2019, destaca que hoy compiten con otros contenidos que pueden ser más atractivos como pueden ser Netflix, Spotify, Apple Music, Amazon Prime, y tienen una diferencia de llegada. Es muy interesante la comparación que realiza de este mercado con lo sucedido en la industria musical, haciendo énfasis en la sustitución de modelos: *"La experiencia de la industria de la música puede ser interesante para entender que el sector de noticias está viviendo una transición análoga y en proceso de transformación hacia un nuevo modelo que muy probablemente le haga retomar su crecimiento. Luego de la época de oro del CD en los '90, la aparición del MP3 y los sistemas de intercambio P2P golpeó sus ingresos entre 2001 y 2010 con una caída del 60%. Sin embargo, durante ese mismo período las ventas digitales comenzaron a crecer sostenidamente gracias al streaming. El cambio de estrategia de la industria se hizo patente en 2014 donde se abrazo el modelo de suscripción y, a partir de allí, ha tenido crecimientos de más del 30% de sus ingresos año a año más que compensando las caídas de ventas físicas y de descargas. En 2018, hubo 255 millones de usuarios de streaming pago haciendo que todo el negocio digital represente el 58.9% total de los ingresos globales de la industria[731]".*

Asimismo, en relación a la disponibilidad de información de calidad, Sebastián Cabello hace referencia al Considerando 55 de la Directiva UE 2019/790 y a un

[729] MARTINEZ, NURIA, "Los fines educativos y de investigación como límite al derecho de autor", DYKINSON, Madrid, 2018, pp. 64.
[730] CABELLO, SEBASTIÁN: "Documento de trabajo N. 2019-4. Centro de Estudios en Tecnología y Sociedad". "La nueva regulación europea de Copyright: ejes clave para el debate en América Latina". Universidad de San Andrés, 2019, URL: http://repositorio.udesa.edu.ar/jspui/bitstream/10908/16695/1/%5BP%5D%5BW%5D%20-%20Cabello%2C%20Sebasti%C3%A1n%20M..pdf Consultado el 20 de enero de 2020.
[731] CABELLO, SEBASTIÁN, obra citada, pp. 11.

informe de la Universidad de Cambridge[732], destacando que la calidad es muy difícil de determinar y que englobar a todos los sitios que encuadren como sitios de noticias es muy discutible[733]. Por el contrario, hace énfasis en que las medidas adoptadas pueden restringir el acceso al contenido, afectando la oferta y la calidad. *"La forma en que se producen, comparten y consumen contenido ha venido cambiando constantemente en internet en tanto ha crecido su proliferación. (...) La falta de estudios empíricos sobre cómo se comportan la oferta y demanda de la industria de bienes sujetos a derechos de autor en el mundo desarrollado hacer pensar que hay que actuar con más cautela todavía en los países en desarrollo, donde el tamaño de las industrias creativas es todavía menor y hay mayores barreras a la entrada.*[734]"

En definitiva, más allá de los desafíos que la nueva Directiva puede implicar para garantizar otro derechos fundamentales, a más tardar el 7 de junio de 2021 los Estados miembros de la Unión Europea deben adoptar las disposiciones legales, reglamentarias y administrativas necesarias para dar debido cumplimiento.

En este sentido, en noviembre de 2019, en España se publicó una consulta pública sobre un borrador de "*Anteproyecto de Ley sobre los derechos de autor y derechos afines en el mercado único digital, por la que se incorporan al ordenamiento jurídico español la Directiva (UE) 2019/789 del Parlamento Europeo y del Consejo de 17 de abril de 2019, y la Directiva (UE) 2019/790 del Parlamento Europeo y del Consejo de 17 de abril de 2019*". De esta forma se busca adaptar la regulación de España en materia de derechos de autor y derechos afines a la realidad del mercado único digital, e incorporar al ordenamiento jurídico español a las nuevas directivas.

Interesa señalar que algunos países, como Alemania, han avanzado en regular los contenidos en Internet, con foco a perseguir la pornografía infantil y la propaganda neonazi. La responsabilidad atiende específicamente a quienes introducen dichos contenidos en la red, no a los proveedores de servicios, salvo que tengan participación en la infracción.

---

[732] University of Cambridge, URL: https://www.cipil.law.cam.ac.uk/sites/www.law.cam.ac.uk/files/images/www.cipil.law.cam.ac.uk/documents/ipomodernisingipprofresponsepresspublishers.pdf
Consultado el 20 de enero 2020.

[733] CABELLO, SEBASTIÁN, obra citada, pp. 12.

[734] CABELLO, SEBASTIÁN, obra citada, pp. 25.

Sin duda estamos ante un gran desafío global, los diversos países están explorando soluciones específicas, a medida, sin limitar más allá de lo necesario para atender el problema concreto.

Es esencial atender la problemática, buscando soluciones a medida, hay que garantizar los derechos de autor sin afectar otros derechos fundamentales.

(IV.6) Consideraciones finales

El gran desarrollo de la tecnología y de Internet tiene gran impacto en los derechos de autor, en tanto la innovación y el desarrollo son fundamentales para el adecuado desarrollo de las empresas y de los países, siendo fundamental atender el tema cabalmente, escuchando y dialogando con todas las partes, para poder responder adecuadamente.

La inteligencia artificial, la robótica y la capacidad de las máquinas de aprender por sí mismas, genera múltiples cuestionamientos relacionados con la propiedad intelectual, que son fundamentales analizar y responder a fin de dar certeza, seguridad y respaldo a la innovación.

Asimismo, el respecto y garantizar los derechos de autor se presenta como fundamental para impulsar la investigación y el desarrollo.

La Unión Europea está trabajando ya desde hace un tiempo sobre la temática, teniendo en cuenta las diversas aristas e imponiendo directrices sobre los países miembros, quienes deben rever sus normativas y hacer cambios para incorporar las mismas en su ordenamiento interno.

En este sentido, España deberá ajustar la LPI a efectos de ajustarse a las nuevas directrices, que contribuirán para promover la investigación, el desarrollo y reflejando la nueva realidad que nos ocupa; al tiempo que deberá atender las futuras directrices que se dicten en relación a la inteligencia artificial y a la robótica.

Uruguay por su parte presenta una norma más amplia, que en principio no parece tener contradicciones, ni afectar el desarrollo, por más que los derechos morales solo se reconocen a personas físicas, no habría límites directos en lo que respecta a la titularidad. Considerando los grandes avances y la necesidad de dar certeza, seguridad y atender la tendencia mundial, será fundamental tener normas actualizadas y

transparentes, a fin de posicionarse como un sitio para el desarrollo de la innovación y la investigación.

V. La seguridad en el mundo digital[735]

(V.1.) Introducción

El buen uso de la tecnología y de Internet tiene grandes beneficios para todos, mas el uso inadecuado puede aparejar grandes daños y límites para la seguridad de las personas, de las empresas, de los gobiernos, así como de las cosas.

Marc Goodman en su libro "*Future Crimes*" comienza haciendo mención a una realidad bastante obvia pero que no siempre consideramos: los criminales continuamente están actualizando las técnicas e incorporando las últimas tecnologías en su *modus operandi*. Innovan y evolucionan sus métodos rápidamente para alcanzar sus objetivos. Se les reconoce como "*early adopters*" de las nuevas tecnologías y del mundo online, lo cual se refleja en que el cibercrimen va en aumento, al tiempo que irrumpe en nuevas y emergentes áreas, como puede ser la robótica, la realidad virtual, la inteligencia artificial, entre otros ejemplos. En este sentido, si bien la tecnología es muy buena, puede ser un arma de doble filo, y cuanto más profundicemos nuestras vidas y cosas en el mundo digital, más asequibles seremos para aquellas personas que saben cómo utilizarlas para afectarnos, si es que no tomamos las medidas adecuadas para protegernos. Vale destacar que en la medida en que todo está conectado, todo es más vulnerable, siendo cada vez más simple poder desestabilizar la seguridad con impacto global[736].

Siguiendo en esta línea, Goodman comenta sobre lo que le ocurrió a Honan, un reportero de San Francisco, quien tenía sus fotos, trabajos, investigaciones, y demás información personal y profesional en su computador, sincronizado automáticamente con su *smartphone*, con su *tablet*, con su nube, con sus cuentas de banco, con sus tarjetas de créditos, etc. Él, como muchos de nosotros, era un blanco fácil para los hackers. Una mañana, sin razón alguna, un hacker irrumpió en su computador, luego en su *smartphone* y demás dispositivos. No solo le hurtó sus fotos, documentos y correos

[735] Véase nuestro trabajo, ARAMENDÍA, MERCEDES, "Seguridad en la era Digital", en *Revista de Derecho y Nuevas Tecnologías*, Número 3, Uruguay, 2020.
[736] GOODMAN, MARC, "Future Crimes. Inside the digital underground and the Battle for Our Connected World", Anchor Books, United States, New York, January 2016, pp. 6 y ss.

electrónicos; sino que además le cambió sus contraseñas y comenzó a utilizar sus redes sociales, como por ejemplo *Twitter* y *Facebook*. De un momento para otro, Honan se encontró imposibilitado de usar su *smartphone*, su computador, de ingresar a sus correos electrónicos y a su nube, donde tenía, entre otras cosas: sus direcciones, su calendario, las fotos de su familia, la información de sus cuentas bancarias, así como información confidencial de su trabajo. Ante la imposibilidad de ingresar a sus redes sociales, Honan se creó otra cuenta en la red social *Twitter* y le preguntó directamente al Hacker por qué le estaba haciendo eso. El Hacker le contestó que no tenía nada personal contra él, simplemente le había gustado el nombre de usuario que utilizaba en *Twitter*[737].

El anterior es un simple ejemplo que permite visualizar que todos, hasta de forma arbitraria, podemos sufrir ese tipo de quiebres en nuestra seguridad, lo cual nos puede generar muchos daños, siendo fundamental ser conscientes y actuar para prevenir y responder en forma y tiempo. A modo de ejemplo, interesa hacer mención al reciente hackeo que sufrió Jeff Bezos, fundador de Amazon, así como que los altos cargos de grandes organizaciones internacionales tienen instrucciones de no utilizar WhatsApp, así como otras aplicaciones populares de mensajería[738].

En pocos años, sin siquiera advertirlo, hemos confiado aspectos fundamentales de nuestras vidas al mundo digital: nuestras direcciones, agendas, fotos, videos, notas, entretenimiento, contraseñas, mensajes, llamadas, correos, etc. Además, muchos constantemente estamos compartiendo en diversas redes sociales nuestras vidas, así como las de nuestros amigos, familiares y compañeros de trabajo. Asimismo, bajamos muchas aplicaciones en las que confiamos para todo: para despertarnos, para hacer ejercicio, para cocinar, para archivar las fotos de nuestros hijos, para llegar a cualquier sitio; y todo, lo hacemos a través de Internet. Al respecto, como promocionaba Apple para iPhone en el año 2009: *"there's an app for that"* (hay una aplicación para eso), para demostrar que había una aplicación de iPhone para prácticamente todas las necesidades humanas[739]. En este sentido, no cabe duda de los beneficios que las aplicaciones y la interconectividad de Internet proveen, facilitando que personas de

[737] Ibídem, pp. 11.
[738] EL PAIS, por qué grandes organizaciones recomiendan no usar Whatsapp. URL: https://elpais.com/tecnologia/2020/01/31/actualidad/1580429952_417173.html Consultado el 31 de enero de 2020.
[739] Ibídem, pp. 75.

todas partes del mundo estén conectadas, permitiendo por ejemplo hasta jugar video juegos en tiempo real con personas que están del otro lado del mundo. Esta interconexión es una de las particularidades que le da más fuerza y utilidad a Internet, pero sin duda tiene riesgos, y la realidad es que cada vez más tenemos toda nuestra vida y nuestros dispositivos conectados globalmente, compartiendo nuestra información, sin cuestionarnos qué implica, qué riesgos tiene, ni qué medidas deberíamos adoptar para mitigarlos[740].

Por otra parte, en Internet lo que viajan son datos, bits, que pasan libremente de un país a otro, sin fronteras o bordes que permitan el contralor, generando problemas de jurisdicción. A modo de ejemplo, se señala un caso ocurrido en el año 1994 donde Vladimir Levin desde su apartamento en Rusia, robó un banco de Nueva York por Internet. Levin hackeo las cuentas de varios clientes, se hizo de $10.7 millones de dólares, y transfirió el dinero a diversas cuentas en Finlandia, Estados Unidos, Holanda, Alemania e Israel. Ante esta situación, las autoridades se plantearon quién tenía jurisdicción en este caso. El ladrón nunca estuvo en Estados Unidos para cometer el crimen, él hizo todo desde su computadora y utilizó un circuito virtual para borrar su huella. Los hackers van a hacer todo para que sus huellas sean difíciles de seguir, y si van a cometer un crimen de un país a otro, probablemente en el medio pasen por otros países, a fin de que su huella sea difícil de rastrear. De esta forma se generan múltiples desafíos y problemas administrativos de jurisdicción.[741]

Además, el desarrollo de la tecnología y de la inteligencia artificial crean nuevas formas que hacen difícil poder identificar lo real de lo que no lo es. A modo de ejemplo, actualmente tenemos personas, correos y voces falsas, en tanto hay diversas aplicaciones que permiten generar cuerpos, caras, voces, correos, etc., que parecen reales pero que no lo son.

Ante todos estos grandes desafíos, tener las herramientas como para darnos cuenta qué es lo real y qué no, es esencial. Además, los quiebres de seguridad toman cada vez más importancia, no solo por los riesgos que puede haber de que nos roben nuestros datos, sino que imaginen si un hacker toma el control de nuestros dispositivos inteligentes o incluso de los sistemas públicos, afectando las infraestructuras críticas, como puede ser la electricidad.

[740] Ibídem, pp. 12 y 13.
[741] Ibídem, pp. 14.

A modo de ejemplo, Goodman cuenta un caso en Polonia donde, sin explicación aparente, de repente un tren dobló para la izquierda, cuando debía girar para la derecha, generando un accidente. Cuando investigaron qué había ocurrido, resultó que un adolescente de catorce años, a modo de juego, había hackeado y creado un sistema remoto capaz de controlar el tránsito de las líneas de la ciudad. Asimismo, en Brasil durante los años 2005 y 2007 diversos incidentes con hackers fueron reportados. En uno de ellos, alrededor de tres millones de personas quedaron en la oscuridad porque el proveedor de energía se negó a responder a las extorciones que se le estaban demandando por ciberdelincuentes[742]. En el mismo sentido, en el año 2007, Estonia fue objeto de un ciberataque desde Rusia, que dejó al país prácticamente *off-line*, y que se conoció como la primer*a ciberguerra*. Desde entonces Estonia se transformó en el país experto en ciberseguridad.[743]

A medida que surgen las amenazas, los antivirus y las respuestas se van actualizando, y los hackers son conscientes de que cuantas más molestias causen en los sistemas, más rápidamente serán detectados. En este sentido, es esencial comprender cómo funciona la tecnología para poder prevenir, aprovechar debidamente las ventajas que nos ofrece, y ser conscientes de que no solo se afecta a particulares y gobiernos, sino que las empresas también están sufriendo gravemente estos atropellos. [744]

Si bien estamos acostumbrados a que los ladrones van tras las tarjetas de crédito para hacer fraudes, así como para robar la identidad de las personas, los datos de seguros de salud, de impuestos, etc. las organizaciones criminales cada vez son más sofisticadas y se han presentado casos en que han hurtado la propiedad intelectual creada por empresas alrededor del mundo. A modo de ejemplo, en octubre de 2013 el sistema de Adobe fue hackeado. No solo le robaron treinta y ocho millones de cuentas, incluyendo nombres de usuario, contraseñas, así como datos de las tarjetas de crédito; sino que además le robaron más de cuarenta gigabytes de código fuente de varios de los productos de la empresa, como ser Acrobat y Photoshop[745].

[742] Ibídem, pp. 26 y 30.
[743] Ibídem, pp. 20-30
[744] Ibídem, pp. 20-30.
[745] Ibídem, pp. 32 y 33.

En este sentido, Matt Karly[746] se refiere al "*Cyber Risk*" (ciberriesgo), haciendo mención al *Institute of Risk Management*, como cualquier riesgo de pérdida financiera, interrupción o daño a la reputación de una organización por algún tipo de falla de sus sistemas de tecnología de la información. Profundiza en qué es un quiebre o falla, y aclara que generalmente son quiebres de seguridad que alcanzan: información de personas, información sensible que puede no estar vinculadas a personas (por ejemplo: propiedad intelectual, información competitiva, secretos comerciales, así como información de terceros), otras formas de ataques como ser un quiebre en las operaciones[747].

A modo de ejemplo, Karly hace mención a cuatro casos ocurridos que implicaron quiebres de seguridad y afectaron a terceros. El primero ocurrió en el 2008 a *Mark & Spencer* quien fue afectado porque su proveedor no protegió la información de sus empleados. El segundo refiere a *Target* en el 2013, en el que hackers utilizaron un proveedor externo de servicios, proveedor de refrigeración, para afectar la red de la empresa, lo cual les implicó perder información personal de 110 millones de compradores. Finalmente, refiere a dos casos ocurridos en el 2017. Uno sufrido por *Equifax*, donde hackers aprovecharon la vulnerabilidad de un proveedor de software externo y accedieron a la información personal de más de 143 millones de personas (número de seguridad sociales, nombres, direcciones, licencias de conducir, etc.). El otro evento mencionado, fue sufrido por *Anthem* (seguro de salud) cuando un empleado de un contratista expuso información personal de más de 18.000 afiliados a sus servicios[748].

En definitiva, las organizaciones criminales evolucionan e innovan constantemente en la forma de delinquir, habiendo distintos tipos de amenazas. Pero el riesgo es constante y puede ser cometido por la acción directa o indirecta de cualquier

[746] KARLYN, MATT, profesor invitado en Cornell Tech, quien dictó el 13 de noviembre de 2019 una clase denominada "*Integrating Information security into de the contracting process*".
[747] Al respecto, interesa comentar un ciberataque sufrido por la empresa Aquajerez en octubre de 2019, el cual obligó a la empresa a cerrar su oficina de atención al cliente hasta que se solucionara el ataque informático. URL: https://www.aqualia.com/es/web/aqualia-global/-/la-oficina-de-aquajerez-cerrada-al-verse-afectada-por-el-ciberataque-al-ayuntamiento Consultado el 20 de enero de 2020.
[748] KARLYN, MATT, fuente citada.

persona que tenga acceso a las redes, facilidades o información, ya sea por medios remotos o físicos[749].

A mero título enunciativo, entre los diversos tipos de ataques, se mencionan que pueden ser realizados por diversas causas, por ejemplo: ciberterrorismo[750], crimen organizado, "*Hactivists*" (activistas que realizan acciones para afectar algo respecto a lo cual están en contra)[751], espionaje comercial e industrial[752], hackeos a empresas por países[753],extorsiones, entre otros múltiples ejemplos[754].

Los ataques pueden ser muy variados, los más comunes son: malware (por ejemplo: virus, troyanos, gusanos, ransomware, spyware), suplantación de identidad (*phishing*), ataques del hombre en el medio (MitM), ataque de denegación de servicios (DOS), inyecciones de código malicioso forzando al servidor a entregar información, vulnerabilidad de día cero, ataque de contraseña, ataques a las cosas conectadas a internet (IoT), entre otros ejemplos[755].

Las modalidades varían y evolucionan continuamente, y así como la tendencia es que la vida de todos es cada vez más digital, es de esperar que los delitos sigan la misma tendencia, siendo esencial la coordinación y el trabajo conjunto a nivel internacional.

Como respuesta, el número de regulaciones y la importancia de la temática va en aumento, con foco en proteger a las personas, así como en el daño que se puede causar por el mal uso de la información, siendo esencial tomar medidas preventivas para

---

[749] Ibídem.

[750] Por ejemplo, el sufrido en el 2016 principalmente por la Costa Este de los Estados Unidos, que impidió ingresar a sitios como CNN, Infobae, New York Times y Twitter, provocando un caos en Internet. URL: https://www.infobae.com/noticias/2016/10/21/un-ataque-hacker-a-un-proveedor-de-internet-en-estados-unidos-afecta-a-twitter-y-spotify/ Consultado el 20 de enero de 2020.

[751] Por ejemplo, los realizados por Anonymous en el año 2011 en Wall Street. URL: https://cybersecuritydegrees.com/faq/the-most-inspiring-cases-of-hacktivism/ Consultado el 20 de enero de 2020.

[752] Cada vez es más sofisticado. Entre los diez principales casos se destacan: el de Moonligjt Maze en 1999, el de Tital Rain desde 2003 al 2005, el Gilette en 1997, así como entre países. URL: https://securityaffairs.co/wordpress/66617/hacking/cyber-espionage-cases.html Consultado el 20 de enero de 2020.

[753][753] Poe ejemplo el hackeo sufrido por Sony en el año 2017 por el cual Estados Unidos sancionó a Korea del Norte. URL: https://www.reuters.com/article/us-cyber-northkorea-sony/u-s-charges-north-korean-hacker-in-sony-wannacry-cyberattacks-idUSKCN1LM20W Consulado el 20 de enero de 2020.

[754] GOODMAN, MARC. Obra citada, pp. 33.

[755] INFOCYTE. Cybersecurity 101: Introducción a los 10 tipos más comunes de ataques de ciberseguridad. URL: https://www.infocyte.com/es/blog/2019/05/01/cybersecurity-101-intro-to-the-top-10-common-types-of-cyber-security-attacks/ Consultado el 25 de enero de 2020.

minimizar las amenazas. En este sentido, se suele hacer foco en la notificación del quiebre de seguridad, en la protección de los datos personales, y en la seguridad nacional, siendo esencial el rol de los proveedores de infraestructura y de los proveedores de servicios digitales[756].

(V.2.) Principios Fundamentales Aprobados por la OCDE[757]

En 1992 la Organización para la Cooperación y el Desarrollo Económico (OCDE)[758] desarrolló las Directrices de Seguridad de los Sistemas de Información. Se revisaron en el año 2001, por el Grupo de expertos de Seguridad de la Información y Protección de la Privacidad, tras la tragedia del 11 de setiembre de dicho año en Estados Unidos.

Destacan que los grandes cambios que se han generado en el entorno tecnológico exigen que los gobiernos, empresas, otras organizaciones, y usuarios que desarrollan, poseen, proporcionan, administran y utilizan estos servicios, pongan atención a los aspectos relacionados con la seguridad. Considerando los grandes cambios generados en la materia, la OCDE aprobó directrices[759], que pretenden atender la seguridad a través del desarrollo de una cultura de seguridad, siendo esencial que se le otorgue un carácter prioritario a la planificación y administración de la seguridad, así como a la comprensión de la temática por parte de todos los participantes de la cadena.

Conforme se señala en las Directrices de la OCDE para la seguridad de sistemas y redes de información, lo que se busca es: (i) Promover una cultura de seguridad de

---

[756] KARLYN, MATT, fuente citada.

[757] Directrices de la OCDE para la seguridad de sistemas y redes de información: Hacia una cultura de seguridad. URL: https://www.oecd.org/sti/ieconomy/34912912.pdf Consultado el 20 de enero de 2020.

[758] Organización para la Cooperación y el Desarrollo Económico (OCDE). Conforme a lo establecido en el artículo 1 del Convenio de la OCDE firmado el 14 de diciembre de 1960 en Paris, la OCDE Tiene por objetivos promover políticas dirigidas a:
A conseguir la mayor expansión de la economía y el empleo y una progresión del nivel de vida en los países miembros, manteniendo la estabilidad financiera, y a contribuir así al desarrollo de la economía mundial.
A contribuir a una sana expansión económica en los países miembros, así como en los países no miembros, en vías de desarrollo económico.
A contribuir a la expansión del comercio mundial sobre una base multilateral y no discriminatoria, conforme con las obligaciones internacionales.
Actualmente son miembros de la OCDE los siguientes países: Alemania, Australia, Austria, Bélgica, Canadá, Chile, Colombia, Corea, Dinamarca, Eslovenia, España, Estados Unidos, Estonia, Finlandia, Francia, Grecia, Hungría, Irlanda, Islandia, Israel, Italia, Japón, Letonia, Lituania, Luxemburgo, México, Noruega, Nueva Zelanda, Países Bajos, Polonia, Portugal, Reino Unido, República Checa, República Eslovaca, Suecia, Suiza, Turquía.

[759] Recomendación del Consejo en su 1037 sesión del 25 de julio de 2002.

proteger los sistemas y las redes de información. (ii) Incrementar la concienciación sobre el riesgo de los sistemas y redes de información; así como sobre las políticas, prácticas, medidas y procedimientos disponibles para poder afrontar dichos riesgos. (iii) Promover una mayor confianza en los sistemas y redes de información. (iv) Crear un marco general de referencia para la comprensión de los aspectos de seguridad, así como de prácticas, medidas y procedimientos. (v) Promover la cooperación y el intercambio de información sobre el desarrollo y ejecución de políticas. (vi) Promover el conocimiento en la materia.

En este sentido, se aprobaron nueve principios, complementarios entre sí y de interés general. Parten de la base de que todos nos veremos beneficiados por la concientización, educación, intercambio de información, capacitación en la seguridad y en las prácticas requeridas; lo cual es fundamental para el desarrollo de una sociedad democrática, así como para contar con flujos de información libres, abiertos y proteger la privacidad de las personas.

Los principios son los siguientes:

- Concienciación: es fundamental comprender la necesidad de contar con sistemas y redes de información seguros, y tener conocimiento de los medios, de los riesgos y de los mecanismos disponibles de salvaguardia.

- Responsabilidad: todos tenemos un rol y debemos comprender nuestra responsabilidad en la seguridad de los sistemas y redes de información locales y globales. Los países deben revisar regularmente sus políticas, prácticas, medidas y procedimientos, y evaluar si son apropiados. Aquellos que desarrollan, diseñan o suministran productos y/o servicios deben elevar la seguridad de los sistemas y redes, y distribuir a los usuarios información para que entiendan la temática, así como la importancia de las actualizaciones.

- Respuesta: todos deben actuar de manera adecuada y conjunta para prevenir, detectar y responder a incidentes que afecten la seguridad. Asimismo, deben compartir información sobre los riesgos y vulnerabilidades, ejecutar procedimientos para una cooperación rápida y efectiva, tanto a nivel nacional como internacional, a fin de prevenir, detectar y responder a incidentes que afecten a la seguridad.

- Ética: se deben respetar los intereses legítimos de terceros, reconociendo que las acciones u omisiones de todos los actores, pueden implicar daños a terceros, siendo esencial desarrollar y adoptar buenas prácticas.

- Democracia: la seguridad debe ser compatible con los valores de una sociedad democrática, como son: la libertad de intercambio de pensamiento e ideas, el libre flujo de información, la confidencialidad de la información y de las comunicaciones, así como la protección de la información personal.

- Evaluar el riesgo: identificar las amenazas y vulnerabilidades, incluyendo factores internos y externos como tecnología, factores físicos y humanos, políticas y servicios de terceros que tengan repercusiones en la seguridad.

- Diseño, ejecución y coordinación de la seguridad como un elemento esencial de los sistemas y redes de información. Las salvaguardas técnicas y no técnicas deben ser proporcionales al valor de la información de los sistemas y redes de información. La seguridad ha de ser un elemento fundamental e integral de todos los productos, servicios, sistemas y redes.

- Gestión de la seguridad: debe estar basada en la evaluación del riesgo y ser dinámica, comprendiendo todos los niveles de las actividades de los participantes y todos los aspectos de sus operaciones. Asimismo, debe incluir posibles respuestas a riesgos emergentes, considerar la prevención, detección y la respuesta a incidentes que puedan afectar la seguridad. Las prácticas, medidas y procedimientos deben estar coordinadas e integrados para crear un sistema coherente de seguridad.

- Reevaluación: constantemente se descubren nuevas amenazas y vulnerabilidades, por lo que es fundamental revisar, evaluar y modificar los aspectos de seguridad continuamente, a fin de poder enfrentar debidamente los riesgos permanentes.

Partiendo de los principios antes expuestos, el 2 de julio de 2003 la OCDE aprobó un Plan de implementación[760]. Por un lado, se reconoce el rol de los gobiernos, y por otro lado se destaca el rol de las empresas y de la sociedad civil.

[760] ORGANIZATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT. Working Party on Information Security and Privacy. Implementation Plan for the OECD guidelines for

En relación con el rol de los gobiernos, se señala que tienen la responsabilidad de proveer liderazgo para el desarrollo de una cultura de seguridad, lo cual incluye el desarrollo de políticas públicas, como propietario, operador y usuario de los sistemas y redes. Asimismo, se destaca la importancia de consultar con otros participantes interesados para el desarrollo de políticas públicas, así como de liderar con el ejemplo en su rol de operador y de usuario de redes.

Como responsable de las políticas públicas es fundamental que desarrollen políticas nacionales de seguridad, al tiempo que cooperen y promuevan una cultura global de seguridad. Entre las iniciativas se mencionan: (i) establecer una serie de medidas legales, de procedimientos y de mutua asistencia para combatir el cibercrimen y asegurar la cooperación transfronteriza; (ii) identificar las unidades nacionales de cibercrimen y puntos de contactos internacionales de asistencia de alta tecnología, y extender dichas capacidades en los casos en que aún no existan; (iii) establecer instituciones de intercambio de amenazas y vulnerabilidades: CERTs (*Computer Emergency Response Teams* o Centros de Respuestas a Incidentes de Seguridad Informática); y (iv) desarrollar cooperación entre los gobiernos y las empresas en el campo de la seguridad de la información y en la lucha contra el cibercrimen.

Además, es importante que realicen esfuerzos que apoyen a todos para alcanzar la seguridad, desarrollando programas e iniciativas para que todos estén atentos y puedan tomar las medidas que correspondan. A modo de ejemplo: asistir para afrontar la seguridad, apoyar la educación y el entrenamiento, establecer puntos de contactos y fuentes de información práctica, remover obstáculos para las acciones de los participantes, así como desarrollar campañas para que se esté consciente de que: (i) los sistemas de información y las redes pueden afectarse tanto por riesgos internos como externos; (ii) las fallas de seguridad pueden afectar significativamente los sistemas y las redes que estén tanto bajo como fuera de su control; (iii) hay potenciales riesgos por la interconectividad y la interdependencia; (iv) es importante entender la configuración y la actualización de los sistemas y de las redes, así como seguir las buenas prácticas para atender la seguridad; (v) se deben adoptar salvaguardias y soluciones para las amenazas y vulnerabilidades conocidas; (vi) se deben desarrollar objetivos de seguridad apropiados para sus necesidades, a fin de prevenir, detectar y responder a las amenazas

---

the security of information system and networks: towards a culture of security. URL: http://www.oecd.org/internet/ieconomy/31670189.pdf Consultado el 20 de enero de 2020.

y vulnerabilidades; (vii) todos deben ser responsables activamente por sus roles individuales; y (viii) se deben revisar las políticas, prácticas, medidas y procedimientos regularmente y evaluar si son apropiadas.

El intercambio de buenas prácticas puede facilitar la habilidad de los usuarios para poder entender y alcanzar los objetivos de seguridad. Además, en el diseño de la seguridad y de los programas de educación, es importante hacer énfasis en la promoción de conductas éticas para reconocer las necesidades de seguridad y respetar los intereses de otros. Asimismo, es primordial que los usuarios sepan como establecer y mantener actualizados los sistemas y las redes. Finalmente, es transcendental el rol de los CERTs, y los puntos para compartir y de analizar información en conjunto con la industria.

Como propietario y operador de sistemas de información y de redes, los gobiernos tienen una responsabilidad especial y deben liderar con el ejemplo, facilitando el desarrollo de buenas prácticas e innovando operacionalmente para beneficiar a todos.

Tienen que: (i) evaluar los riesgos, el diseño y la implementación de seguridad, gestionar la seguridad y reevaluarla. (ii) Desarrollar políticas que reflejen las mejores prácticas para el manejo de la seguridad y del riesgo. (iii) Identificar las amenazas y las vulnerabilidades para manejar los factores internos y externos, como pueden ser: la tecnología, factores humanos y físicos, políticas y servicios de terceros que tengan impacto en la seguridad. (iv) Manejar la seguridad de forma dinámica, abarcar diversos niveles y actividades del gobierno, comprender las amenazas emergentes y prevenir, detectar y responder a los incidentes, así como realizar mantenimiento de forma continuo, revisando y controlando, a fin de coordinar y crear sistemas coherentes. (v) Reconocer los estándares internacionales ISO (Organismo Internacional de Normalización) a fin de establecer sistemas de seguridad efectivos.

Con relación al rol de las empresas y de la sociedad civil, se destaca que tienen un doble rol: (i) como propietarios y operadores, y (ii) como usuarios.

Como propietarios y operadores, al igual que los gobiernos, deben: (i) evaluar los riesgos, diseñar e implementar la seguridad, gestionarla, así como reevaluarla; (ii) gestionar la seguridad en base a los riesgos; (iii) identificar las amenazas y vulnerabilidad teniendo en cuenta factores internos y externos; (iv) dialogar constantemente con los diversos actores del sector; (v) garantizar que los productos y servicios reflejen las prácticas de seguridad; (vi) desempeñar un rol de liderazgo en el

desarrollo de estándares internacionales, incluyendo la participación en actividades de organismos de normalización como son el ISO y el IETF (Internet Engineering Task Force).

Como usuarios, deben asegurarse y usarlos teniendo en cuenta las guías de la OCDE, principalmente el diseño, la implementación y la gestión, contribuyendo con la seguridad global.

Teniendo en cuenta lo anterior, el 16 de diciembre de 2005 la OCDE publicó el paper Número 102 relacionado con la Economía Digital, denominado *"The Promotion of a Culture of Security for Information Systems and Networks in OECD Countries"*[761] (La promoción de una cultura de seguridad para los sistemas y redes de información en los países de la OCDE). Se da cuenta de las diversas acciones que los países que integran la OCDE están implementando, y se identificaron dos principales motores para el desarrollo de una cultura de seguridad.

El primer motor: lo constituyen las aplicaciones de gobierno electrónico y servicios para optimizar las operaciones, ofreciendo mejores servicios a los ciudadanos. Se comprende a la seguridad de una forma cabal, desde el ámbito de la tecnología, de la prevención y de la gestión de riesgos, concientizando a los usuarios. En algunos casos se ha requerido al sector privado y a los ciudadanos que implementen controles de seguridad, dentro de sus sistemas y redes, para poder acceder de forma segura a los servicios del gobierno y para intercambiar datos. De esta forma, se les proporciona orientación, mejores prácticas e información sobre la seguridad, al tiempo que se les invita a conferencias y talleres para capacitarlos e informarlos sobre los problemas vinculados con la materia.

El segundo motor: es la protección nacional de la infraestructura crítica, como por ejemplo la de energía, agua, transporte, sector financiero, telecomunicaciones, servicios sanitarios. Se busca evitar cualquier interrupción en su funcionamiento, siendo esencial el diálogo entre la industria y el gobierno, mediante el establecimiento de asociaciones público-privado y el intercambio de buenas prácticas y de información. En el caso de Estados Unidos, se identifican los siguientes sectores de infraestructura crítica: químico;

[761] OECD Digital Economy Papers No. 102: The Promotion of a Culture of Security for Information Systems and Networks in OECD Countries. URL: https://www.oecd-ilibrary.org/docserver/232017148827.pdf?expires=1579684789&id=id&accname=guest&checksum=5DA1786E44A7AE2307B088EF3858CC8B Consultado el 20 de enero de 2020.

instalaciones comerciales; comunicaciones; fabricación crítica; presas/represas; base industrial de defensa; servicios de emergencia; energía; servicios financieros; comida y agricultura; instalaciones gubernamentales; salud; tecnología de información; reactores nucleares, materiales y residuos; sistemas de transporte; sistemas de agua y aguas residuales[762].

Finalmente, la legislación nacional sobre privacidad se presenta como un motor indirecto, principalmente por la necesidad de proteger los datos personales y la privacidad, así como de cumplir con los requisitos legales.

En general las políticas nacionales que se han desarrollado en la materia han sido el resultado de un enfoque multidisciplinario y del trabajo conjunto entre múltiples partes interesadas. No basta con un enfoque técnico, sino que se requiere considerar aspectos socioeconómicos y legales. Además, ha sido fundamental que las políticas naciones estén respaldadas al más alto nivel gubernamental para su efectiva implementación, y se destaca el rol de la cooperación internacional como un factor fundamental para luchar contra el cibercrimen, así como establecer redes operativas donde intercambiar información y mejores prácticas.

En definitiva, entre los aspectos que mayoritariamente se están considerando, se destacan:

- combatir el cibercrimen: para lo cual muchos países han ajustado sus legislaciones y han establecido organismos coordinadores, que cooperan con el sector privado y a nivel internacional, al tiempo que trabajan para concientizar a la sociedad.

- Establecer CERTs, encargados, entre otras cosas, de atender las necesidades de organizaciones públicas y privadas, de intercambiar información y asesoramiento, así como de cooperar internacionalmente.

- Crear conciencia sobre la necesidad de una cultura de seguridad, para lo cual se desarrollan eventos, seminarios, talleres y conferencias públicas, se

[762] Homeland Security, Sectores de infraestructura crítica: https://www.dhs.gov/cisa/critical-infrastructure-sectors referenciado en OEA-AWS-Marco NIST de ciberseguridad, URL: https://www.oas.org/es/sms/cicte/docs/OEA-AWS-Marco-NIST-de-Ciberseguridad-ESP.pdf Consultado el 20 de enero de 2020.

distribuye información, se brindan recomendaciones, mejores prácticas, orientación, y se da participación al sector privado y a los ciudadanos.

- Educación: se utilizan diversos canales educativos para difundir sobre la seguridad de la información y los sistemas de red, así como formar a los maestros y profesores en tanto son esenciales para multiplicar la transmisión de la información y del conocimiento.

Entre las áreas que se deben desarrollar y que al momento están recibiendo menos atención, se destacan: la investigación y el desarrollo, la evaluación y valoración, y alcanzar a las pequeñas y medianas empresas.

(V.3.) Ciberseguridad en Uruguay

Más allá de diversas disposiciones vinculadas con el ámbito legal, se destacan los siguientes instrumentos:

(V.3.A) Decretos números 451/2009, 452/2009 y 92/2014.

El artículo 73 de la Ley 18.362 crea el "Centro Nacional de Respuesta a Incidentes de Seguridad informática" (CERTuy) en la Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento (AGESIC). El funcionamiento y la organización de CERTuy se estableció en el Decreto número 451/2009. Posteriormente, el artículo 149 de la Ley 18.719 creó, dentro de la AGESIC, la Dirección de Seguridad de la Información que alberga al CERTuy.

CERTuy protege los sistemas informáticos que soportan activos de información críticos del Estado. Se define como un equipo de respuesta y un centro de coordinación de emergencias informáticas[763].

Se entiende por "sistemas informáticos" a "*los ordenadores y redes de comunicación electrónica así como los datos electrónicos almacenados, procesados, recuperados o transmitidos por los mismos para su operación, uso, protección y mantenimiento*[764]", y por "activos de información críticos del Estado" a "*aquellos activos de información necesarios para asegurar y mantener el correcto funcionamiento de los servicios vitales para la operación del gobierno y la economía*

[763] AGESIC: MARCO DE CIBERSEGURIDAD 4.0, URL: https://archivos.agesic.gub.uy/nextcloud/index.php/s/cgbssgiLEopFcRm#pdfviewer Consultado el 20 de enero de 2020.
[764] Artículo 3, d) del Decreto 451/2009.

del país.[765]", como son "*los servicios referidos a la salud, orden público, servicios de emergencia, energía, telecomunicaciones, transporte, suministro de agua potable, ecología y ambiente, agroindustria, servicios públicos, banca y servicios financieros o cualquier otro servicio que afecte a más del 30% de la población*"[766].

Conforme lo establecido en el artículo 4 del Decreto número 451/2009, al CERTuy le compete:

"a) Asistir en la respuesta a incidentes de seguridad informática a los organismos estatales afectados.

b) Coordinar con los responsables de la seguridad de la información de los organismos estatales para la prevención, detección, manejo y recopilación de información sobre incidentes de seguridad informática.

c) Colaborar y proponer normas destinadas a incrementar los esfuerzos con la finalidad de aumentar los niveles de seguridad en los recursos y sistemas relacionados con las Tecnologías de la Información y la Comunicación (TIC) en el Estado.

d) Asesorar y difundir información para incrementar los niveles de seguridad de las TIC, desarrollar herramientas, técnicas de protección y defensa de los organismos.

e) Alertar ante amenazas y vulnerabilidades de seguridad en sistemas informáticos de los organismos.

f) Realizar las tareas preventivas que correspondan.

g) Coordinar planes de recuperación de desastres y realizar un análisis forense del incidente de seguridad informática reportado.

h) Centralizar los reportes y llevar un registro de toda la información sobre incidentes de seguridad informática ocurridos en sistemas informáticos del Estado y reportados al CERTuy.

i)Fomentar el desarrollo de capacidades y buenas prácticas, así como la creación de equipos de respuesta ante incidentes de seguridad informática (CSIRT) para mejorar el trabajo colaborativo.

j) Interactuar como único interlocutor nacional en las comunicaciones con organismos nacionales e internacionales de similar naturaleza.

[765] Artículo 3, b) del Decreto 451/2009.
[766] Artículo 3, e) del Decreto 451/2009.

El artículo 149 de la Ley 18.719, agregó entre los cometidos, asesorar en la definición de políticas, metodologías y buenas prácticas en seguridad de la información en la Administración Pública, así como brindar apoyo en las etapas de implementación.

Interesa destacar la División Centro de Operaciones de Ciberseguridad (SOC), la cual cómo surge de la página institucional de AGESIC, tiene como objeto analizar y procesar múltiples fuentes de datos, para predecir, prevenir, detener y analizar incidentes de seguridad informática[767]. Entre sus cometidos se señalan los siguientes: (i) asesorar en la definición de políticas, metodologías y buenas prácticas en operaciones ciberseguridad; (ii) monitorear los sistemas informáticos que soportan activos de información críticos del Estado; (iii) operar infraestructura de ciberseguridad del Estado; (iv) colectar y analizar la información histórica de ciberseguridad; (v) coordinar el relacionamiento con partes interesadas en ciberseguridad de seguridad de la información; (vi) interactuar con CERTuy y otros CSIRTs para intercambiar información; y (viii) Interactuar con otros SOC, locales e internacionales, intercambio de información y alertas de ciberseguridad[768].

E Decreto número 92/2014 reglamenta el artículo 149 de la Ley 18.719 previendo que: (i) los organismos de la Administración Central deben utilizar nombres de dominio ".gub.uy" y el Ministerio de Defensa: ".mil.uy"; (ii) asimismo deben utilizar correos electrónicos institucionales con nombre de dominio ".gub.uy" o ".mil.uy", también sus funcionarios en el ejercicio de sus funciones; y (iii) los sistemas informáticos de la Administración Central deben estar alojados en centros de datos seguros en territorio nacional, salvo aquellos que no constituyan un riesgo para el organismo.

El artículo 55 de la Ley 18.046, con la redacción dada por el artículo 118 de la Ley 18.172, en materia de seguridad en el uso de las tecnologías de la información y las comunicaciones en el Estado, le confiere a la AGESIC la misión de "*impulsar el avance de la sociedad de la información y del conocimiento, promoviendo que las personas, las empresas y el Gobierno realicen el mejor uso de las tecnologías de la información y las comunicaciones".* Así como para *"promover el establecimiento de seguridades que*

[767] https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/tramites-y-servicios/servicios/centro-de-operaciones-de-seguridad-soc Consultado el 31 de enero de 2020.

[768] https://www.gub.uy/centro-nacional-respuesta-incidentes-seguridad-informatica/institucional/cometidos/division-centro-de-operaciones-de-ciberseguridad-soc Consultado el 31 de enero de 2020.

hagan confiable el uso de las tecnologías de la información", debiendo *"concebir y desarrollar una política nacional en temas de seguridad de la información, que permitan la prevención, detección y respuesta frente a incidentes que puedan afectar los activos críticos del país".*

En ese sentido, el artículo 74 de la ley 18.362 faculta a la AGESIC a "apercibir directamente a los organismos que no cumplan con las normas y estándares en tecnología de la información establecidas por la normativa vigente, en lo que refiera a seguridad de los activos de la información, políticas de acceso, interoperabilidad e integración de datos".

Considerando lo anterior, el Decreto número 452/2009 dispone que las Unidades Ejecutoras de los Incisos 02 al 15 del Presupuesto Nacional (Presidencia de la República y los Ministerios) deben adoptar una Política de Seguridad de la Información, en base a la "Política de Seguridad de la Información para Organismos de la Administración Pública", que se establece en el Anexo I del Decreto. Además, se exhorta a los Gobiernos Departamentales, Entes Autónomos, Servicios Descentralizados y a todos los órganos del Estado a adoptar las disposiciones establecidas en el Decreto.

Vale mencionar el artículo 158.B de la Ley 18.719 que, respecto al intercambio de información señala que los sujetos involucrados deben cumplir con las obligaciones de secreto, reserva o confidencialidad, así como adoptar las medidas necesarias para garantizar niveles adecuados de seguridad y confidencialidad.

En la misma línea, el artículo 159 de la Ley 18.719 prevé que el intercambio de información entre entidades públicas, estatales o no, debe ajustarse a los siguientes principios: cooperación e integralidad, finalidad, confianza y seguridad, previo consentimiento informado de los titulares de los datos personales, eficiencia y eficacia.

El Decreto número 178/2013 reglamenta los artículos 157 a 160 de la Ley 18.719. En el artículo 2 dispone el deber de toda Entidad Pública de intercambiar información pública que produzca, obtenga, obre en su poder o se encuentre bajo su control, con cualquier otra Entidad Pública que así se lo solicite. Respecto a la información privada, requiere el consentimiento libre, previo, expreso e informado del titular de los datos[769]. Interesa señalar que, tanto durante el intercambio de la información como en el

[769] Artículo 3 del Decreto número 178/2013.

procesamiento de esta, se deben adoptar las medidas que sean necesarias para garantizar la seguridad conforme las políticas, estándares, buenas prácticas y normas técnicas que dicte AGESIC. En esta línea, se prevé que AGESIC pondrá a disposición de las Entidad Públicas una Plataforma de Interoperabilidad, por medio de la cual podrán intercambiar la información en soporte electrónico, de forma segura y confiable.

(V.3.B) Protección de Datos Personales, Ley 18.331.

La protección de los datos personales se reconoce como un derecho inherente a la personalidad humana. La protección comprende todo dato personal que esté registrado en cualquier soporte que lo haga susceptible de tratamiento, y a toda modalidad de uso posterior, ya sea en el ámbito público o privado, reconociendo excepciones como ser las que tenga por objeto la seguridad pública, la defensa, la seguridad del Estado y sus actividades en materia penal, investigación y represión del delito. [770].

Los artículos 5.E) y 10 de la Ley 18.331 disponen el principio de seguridad de los datos. Se prevé que el responsable[771] o usuario[772] de la base de datos, debe adoptar las medidas que resulten necesarias para garantizar la seguridad y confidencialidad de los datos personales, a fin de evitar su adulteración, pérdida, consulta o tratamiento no autorizado, así como detectar desviaciones de información intencionales o no. Los datos deben estar almacenados de modo que permitan el ejercicio del derecho de acceso a su titular. Por otra parte, se prohíbe el registro de datos personales en bases de datos que no reúnan condiciones técnicas de integridad y seguridad.

Por otra parte, el artículo 12 de la Ley 18.331, en la redacción dada por el artículo 39 de la Ley 19.670, prevé el principio de responsabilidad, conforme al cual el responsable de la base de datos o tratamiento y el encargado, en su caso, deben ejercer una responsabilidad proactiva y adoptar las medidas apropiadas, como ser: privacidad desde el diseño, privacidad por defecto, evaluación de impacto a la protección de datos, entre otras, a fin de garantizar un tratamiento adecuado de los datos personales y demostrar su efectiva implementación.

---

[770] Artículo 3 de la Ley 18.331.
[771] Artículo 4, k), de la ley 18.331: Es responsable toda *"persona física o jurídica, pública o privada, propietaria de la base de datos o que decida sobre la finalidad, contenido y uso del tratamiento".*
[772] Artículo 4, N), de la ley 18.331:*"toda persona, pública o privada, que realice a su arbitrio el tratamiento de datos, ya sea en una base de datos propia o a través de conexión con los mismos".*

Además, el artículo 20 de la Ley 18.331 prevé expresamente el deber de los operadores que explotan redes públicas o que presten servicios de comunicaciones electrónicas de garantizar la protección de los datos personales. Asimismo, se establece que deben adoptar las medidas técnicas y de gestión adecuadas para preservar la seguridad en la explotación, y que, en caso de riesgo concreto de violación de la seguridad, el operador debe informar a los abonados sobre dicho riesgo, así como sobre las medidas a adoptar.

Interesa destacar el artículo 25 de la Ley 18.331 que trata sobre las bases de datos correspondientes a las Fuerzas Armadas, Organismos Policiales o de Inteligencia. En tanto señala que el tratamiento de los datos personales, con fines de defensa nacional o seguridad pública, sin previo consentimiento de los titulares, se limita a aquellos supuestos y categorías de datos que sean necesarios para el estricto cumplimiento de las misiones legalmente asignadas para la defensa nacional, la seguridad pública o para la represión de los delitos. En dicha línea, dispone que los datos personales registrados con fines policiales deben ser cancelados cuando no sean necesarios para las averiguaciones que motivaron el almacenamiento.

(V.3.C) Marco de Ciberseguridad de Uruguay (MCU)[773]

AGESIC aprobó la versión 4.0 en enero del 2018 del MCU, el cual se presenta como un conjunto de requisitos necesarios para la mejora de la seguridad de la información y la ciberseguridad, que permite a las organizaciones alinear sus procesos de gestión de seguridad informática a nivel internacional.[774]

El MCU es adaptable a diferentes realidades e industrias, y puede ayudar a una organización a planificar y desarrollar su estrategia de gestión de riesgos de ciberseguridad, en función de sus características. Se basa en el Marco definido por el Instituto Nacional de Estándares y Tecnologías (NIST o *National Institute of Standards and Technology*), a efectos de dar respuesta a las amenazas cibernéticas, la gestión de los riesgos y de la seguridad. Está alineado con las mejores prácticas internacionales,

[773] AGESIC: MARCO DE CIBERSEGURIDAD 4.0, URL: https://archivos.agesic.gub.uy/nextcloud/index.php/s/cgbssgiLEopFcRm#pdfviewer Consultado el 20 de enero de 2020.

[774] La primera versión es de agosto de 2016, la segunda de noviembre de 2016, la tercera de junio de 2017, y la cuarta es de enero 2018.

como ISO/IEC 27001:2013, COBIT 5 para Seguridad de la Información y NIST SP 800.-53 rev.4.[775]

El MCU se basa en el ciclo de vida del proceso de gestión de la ciberseguridad desde el punto de vista técnico y organizacional. Se divide en funciones, categorías y subcategorías. Cada una de las subcategorías tiene asociada referencias a normas y estándares de seguridad internacionales, además se le agregaron prioridades, se elaboraron y asignaron requisitos siguiendo la norma ISO/IEC 27001:2013, la normativa vigente y las mejores prácticas internacionales en materia de seguridad de la información[776].

Del ciclo de vida de la ciberseguridad, se extraen los principales conceptos y funciones de la seguridad de la información:

- Identificar: comprender el contexto de la organización, de los activos que soportan los procesos críticos y los riesgos asociados. Definir los recursos y las inversiones en base a la estrategia de gestión de riesgos y a los objetivos. Entre las subcategorías, se encuentra la gestión de activos, lo cual implica identificar y gestionar los datos, dispositivos, sistemas e instalaciones de la organización en base a los objetivos y a la estrategia de riesgo.

- Proteger: los procesos y los activos de la organización. Entre las subcategorías, se comprende el control de acceso a los activos e instalaciones, procesos o dispositivos, actividades y transacciones.

- Detectar: las actividades necesarias para identificar de forma temprana los incidentes de seguridad. Entre las subcategorías, se comprende descubrir actividades anómalas de forma oportuna y el potencial impacto de los eventos.

- Responder: para tomar medidas en caso de un evento o incidente de seguridad, a fin de reducir el impacto. Entre las subcategorías, se destaca la planificación de la respuesta, que implica que los procesos y procedimientos de respuesta se ejecuten y mantengan garantizando una respuesta oportuna para detectar eventos de ciberseguridad.

---

[775] AGESIC: MARCO DE CIBERSEGURIDAD 4.0, URL: https://archivos.agesic.gub.uy/nextcloud/index.php/s/cgbssgiLEopFcRm#pdfviewer Consultado el 20 de enero de 2020.

[776] Ibídem.

- Recuperar: implica la gestión para restaurar los procesos y servicios afectados por un incidente de seguridad. Entre las subcategorías, se destaca la planificación de la recuperación, ejecución y mantenimiento de procesos y procedimientos de recuperación para asegurar la restauración oportuna de los sistemas o activos afectados por eventos de ciberseguridad.

Se establece una Guía de Implementación con los requisitos mínimos para implantar un Sistema de Gestión de Seguridad de la Información, en base a las mejores prácticas internacionales.

Entre los requisitos, conforme a lo establecido en el Marco de Ciberseguridad 4.0., se encuentran los siguientes:

- Gestión de riesgos: la organización debe desarrollar un proceso de evaluación y tratamiento de riesgos de seguridad y, de acuerdo con su resultado, implementar las acciones correctivas y preventivas correspondientes, así como elaborar y actualizar el plan de acción. El objetivo es contribuir con la seguridad de la información, prevenir o reducir los efectos no deseados y lograr la mejora continua[777].

- Planificación: establecer la estrategia de seguridad de la información mediante objetivos claros en plazos anuales, alineados a la estrategia de la organización.

- Política de Seguridad de la Información: para establecer medidas que garanticen la confianza y seguridad de los sistemas y de la información en poder de la organización, así como para proteger los activos de información y minimizar el impacto en los servicios causados por amenazas o incidentes de seguridad.

- Organización: designar un responsable de la seguridad de la información, así como conformar un comité de seguridad de la información formado por personas con capacidad de decisión sobre los objetivos de la organización, que vele por la seguridad de la información, marque los lineamientos estratégicos en la materia y defina los objetivos anuales. Asimismo, definir los mecanismos para el contacto formal con autoridades y equipos de respuesta, y abordar la

[777] Ibídem.

seguridad de la información en la gestión de los proyectos desde su inicio, independientemente del tipo de proyecto. Además, establecer el uso de dispositivos móviles, así como establecer los controles para proteger la información a la que se accede de forma remota, tanto por personal interno como externo, garantizando la seguridad de la información.

- Gestión humana: establecer acuerdos con el personal donde figuren sus responsabilidades y de las organizaciones, buscando que comprendan y tomen conciencia de sus responsabilidades, y apliquen la seguridad de acuerdo con las políticas y procedimientos establecidos.

- Gestión de activos: identificar los activos de la organización y su responsable, garantizando su gestión. Clasificar y proteger la información de acuerdo con la normativa y a los criterios de valoración definidos. Asimismo, pautar el uso aceptable de los activos y gestionar los medios de almacenamiento. Por otra parte, establecer los mecanismos para destruir la información y los medios de almacenamiento.

- Control de acceso: gestionar y autorizar el acceso lógico a los activos de información, revisar los privilegios de acceso, establecer controles criptográficos para proteger la confidencialidad, autenticidad e integridad de la información digital, y disponer controles para el uso de firma electrónica.

- Seguridad física y del ambiente: implementar controles de acceso físico a las instalaciones y equipos ubicados en los centros de datos y áreas relacionadas. Así como controles ambientales en los centros de datos y áreas relacionadas. Además, contar con un sistema de gestión y monitoreo centralizado capaz de alertar fallas en componentes críticos.

- Seguridad de las operaciones: gestionar las vulnerabilidades técnicas, a fin de prevenir y mitigar el riesgo de explotación de vulnerabilidades técnicas en los sistemas, así como los cambios para que no comprometan la seguridad. Incluye, gestionar la capacidad de los servicios y recursos que se encuentren operativos para que puedan cumplir con los objetivos acordados de capacidad y desempeño. Además, requiere definir entornos separados para reducir los riesgos de acceso no autorizado, evitando modificaciones no deseadas de archivos o sistemas, y fallas en los sistemas. Por otra parte, también requiere asegurar la

protección contra software malicioso, por ejemplo: virus, gusanos, troyanos, spyware, entre otros. En este sentido, es también requisito respaldar la información y realizar pruebas de restauración periódicas para preservar la información de la organización o en su poder, y restaurarla en tiempo y forma en caso de que sea necesario. Finalmente, demanda registrar y monitorear los eventos de los sistemas para asegurar la protección de los registros de eventos contra modificaciones y/o accesos no autorizados y asegurar los registros de auditoria; así como gestionar la instalación de software para garantizar la integridad y seguridad de los sistemas.

- Seguridad de las comunicaciones: requiere que los portales web de los organismos de la Administración Central y sus dependencias se identifiquen debidamente. Se prevé que los nombres de dominio del organismo o dependencia sea sus iniciales, su acrónimo o el nombre por el que se le conozca, buscando que sea la más representativa. Se requiere se comunique a AGESIC la información de contacto del responsable de los dominios y subdominios, y actualizarse cada seis meses. Además, se requiere establecer acuerdos de no divulgación, y que los servidores de dominio gubernamentales se alojen dentro del territorio nacional, y no se permite su implantación sobre tecnologías que no garanticen dicho requerimiento. Por otra parte, se exige la implementación de canales cifrados utilizando protocolos seguros para el intercambio entre servidores ug.uy. Cuando la comunicación sea con terceros, se procurará que sea cifrado, pero cuando no sea posible se podrá establecer un canal de texto claro, tratando de conservar la confidencialidad de los datos

- Adquisición, desarrollo y mantenimiento de los sistemas: requiere incluir requisitos de seguridad de la información durante todo el ciclo de vida de los proyectos de desarrollo o adquisiciones de software.

- Relación con proveedores: requiere definir acuerdos de niveles de servicios (SLA) con los proveedores de servicios críticos que permitan nivelar las expectativas y responder con la calidad y en los tiempos establecidos. Además, pide establecer pautas, realizar seguimiento y revisión de los servicios de los proveedores y gestionar sus cambios.

- Gestión de incidentes: exhorta a planificar la gestión de los incidentes de seguridad de la información, y contar con mecanismos que permitan evaluar los eventos, decidir si se clasifican como incidentes de seguridad de la información, identificar el impacto y el alcance. Por otra parte, requiere informar de forma completa e inmediata la existencia de un potencial incidente de seguridad informática al CERTuy o equipo de respuesta externo correspondiente, así como registrar y reportar los incidentes para evaluarlos, estudiarlos, contar con estadísticas y tomar las acciones necesarias en forma rápida y efectiva siguiendo los procedimientos correspondientes establecidos. En la misma línea, se quiere responder ante incidentes de seguridad de la información de forma coordinada, rápida y efectiva, asegurando que se pueda reanudar el nivel de seguridad normal para posteriormente dar comienzo a la recuperación, conforme a los mecanismos de recuperación establecidos.

- Continuidad de las operaciones: requiere contar con componentes redundantes que contribuyan al normal funcionamiento del centro de datos y operaciones, y asegurar que la infraestructura de redes de telecomunicaciones tenga redundancia para que el centro de datos pueda continuar operando aun ante la caída de un activo de red, garantizando la continuidad y la recuperación de las operaciones. Por otra parte, requiere definir métricas básicas para planificar la continuidad de las operaciones, así como los mecanismos de comunicación e interlocutores válidos.

- Cumplimiento normativo: requiere asegurar el cumplimiento normativo relacionado con la seguridad de la información y con los requisitos de seguridad, así como realizar auditorías independientes para asegurar la conveniencia, adecuación y eficacia continua de la gestión de la información en la organización conforme al Marco de ciberseguridad. Por otra parte, demanda revisar los sistemas de información mediante pruebas de intrusión (*ethical hacking*), evaluar las vulnerabilidades y gestionar las licencias de software.

Interesa señalar que en el 2019 se publicó la Edición 5 de Ciberseguridad, Marco NIST: *"Un abordaje integral de la Ciberseguridad",* realizado por la Organización de Estados Americanos (OEA) y AWS, donde se hace mención: (i) al marco normativo NIST de ciberseguridad (CSF), su historia, estructura, funciones y evolución; (ii) a la

estrategia para adoptar el CSF y los principales desafíos; y (iii) a dos casos de estudio: Reino Unido que da un enfoque abierto, y Uruguay con un enfoque guiado. [778]

A modo de introducción, interesa señalar que el CSF (Cybersecurity Framework) nació como consecuencia de que, en febrero de 2013, tras el aumento sostenido de la cantidad de incidentes de ciberseguridad en los Estados Unidos, Barack Obama ordenó al Instituto Nacional de Estándares y Tecnologías (NIST) el desarrollo de un Marco de ciberseguridad para la protección de la infraestructura crítica. Fue desarrollado y promovido con el aporte de todas las partes interesadas (gobierno, la industria y la academia). Busca una amplia difusión y talleres para: (i) identificar las normas de ciberseguridad existentes, directrices, marcos y buenas prácticas, (ii) especificar brechas de alta prioridad para las que se necesitaban nuevos estándares; y (iii) desarrollar planes de acción en colaboración.[779]

En este sentido, el CSF es una herramienta para la gestión de riesgos de ciberseguridad, que habilita la innovación tecnológica y se ajusta a cualquier tipo de organización, tomando como estrategia basarse en estándares ya aceptados por la industria. Agrupa los controles establecidos por los principales estándares de la industria, internacionalmente reconocidos como con NIST SP 800-53, ISO 27001, COBIT 5, entre otros; y actualmente es reconocido por la comunidad técnica como el marco que contempla las mejores prácticas en lo que refiere a la ciberseguridad y algunos países lo han incluido como legislación nacional, aunque con diferentes enfoques. [780]

En el caso de Reino Unido, definido como un enfoque abierto, cuenta con un Marco de Políticas de Seguridad obligatorio para todos los departamentos de gobierno, y se han desarrollado diversas guías para el cumplimiento, dentro de los cuales se encuentra el Estándar Mínimo de Ciberseguridad (MCSS – *Minimum Cyber Security Standard*). El MCSS define las medidas de seguridad mínimas que deben implementar para proteger la información, tecnología y servicios digitales; pero deja abierta la

[778] OEA Y AWS, Ciberseguridad, Marco NIST. URL: https://www.oas.org/es/sms/cicte/docs/OEA-AWS-Marco-NIST-de-Ciberseguridad-ESP.pdf Consultado el 20 de enero de 2020, pp. 3.
[779] Ibídem, pp. 4.
[780] Ibídem, pp. 7

implementación de los lineamientos, alentando a que las empresas interpreten el estándar de forma independiente y adopten sus propios procesos. [781]

El caso de Uruguay, definido como un enfoque guiado para cualquier organización, que no es de adopción obligatoria. Se comenta que, si bien el MCU se basa en el NIST, implementa solo un núcleo de subcategorías, con el fin de facilitar el abordaje y la elaboración de planes de acción, e incorpora requisitos propios a partir de los controles ISO/IEC 27001 y la normativa uruguaya de ciberseguridad.[782]

La OEA concluye su informe señalando que los programas de ciberseguridad más exitosos son los que definen una estrategia para abordar cada una de las funciones esenciales de ciberseguridad, siendo fundamental una visión holística: personas, procesos y tecnología.[783]

(V.3.D) Recomendaciones de Seguridad en IoT (Internet de las Cosas).

Durante el 2019, AGESIC junto con Internet Society realizaron en Uruguay el proceso de trabajo *multistakeholder* para generar recomendaciones vinculadas con Seguridad en IoT, las cuales fueron presentadas en noviembre de 2019 en la cumbre del D9 celebrada en Uruguay.

Se parte de la base de que la naturaleza abierta de Internet crea la habilidad de conectar diversos dispositivos, sistemas, aplicaciones y servicios de una forma que transforma la manera en que se interactúa, y se destaca el impacto que va a tener IoT para mejorar el mundo, así como los múltiples sectores de actividad en los cuales los sistemas y/o dispositivos se diseñan, crean, desarrollan y ponen en el mercado. Se define IoT tomando la definición de la Unión Internacional de Telecomunicaciones (UIT o ITU) como: *"una infraestructura global al servicio de la Sociedad de la Información, que propicia la prestación de servicios avanzados mediante la interconexión (física y virtual) de las cosas, gracias a la interoperabilidad de Tecnologías de la Información y la Comunicación presentes y futuras. Además, gracias a la identificación, la adquisición y el procesamiento de datos, así como a las capacidades de comunicación, IoT hace uso de las cosas para ofrecer servicios a todo*

[781] Ibídem, pp. 9
[782] Ibídem, pp. 10
[783] Ibídem, pp. 12.

tipo de aplicaciones, garantizando, a su vez, el cumplimiento íntegro de los requisitos de seguridad y privacidad."[784]

Destaca que IoT cambia rápidamente, en tanto constantemente se descubren nuevas habilidades y nuevos problemas de seguridad, además de que las soluciones que se van presentando son emergentes y de actualización constante en tanto se está analizando globalmente la temática[785].

Se identifican múltiples desafíos sobre los cuales se debe trabajar, y se presentan dos vías de acción: (1) proteger a los consumidores, y (2) alcanzar resiliencia en la red.[786]

Respecto a la protección del consumidor, se entiende fundamental generar confianza y reglas claras en el ecosistema para facilitar el desarrollo y la innovación, impulsando la universalización y la masificación de los sistemas y/o dispositivos en un contexto seguro. Se identifican los principales objetivos, como ser que las personas puedan identificar el nivel de seguridad de los sistemas y/o dispositivos, que consideren los términos y condiciones, que reciban y actualicen los sistemas, y que tomen medidas para atender su privacidad y proteger su información.[787]

Asimismo, se identifican los diversos aspectos sobre los cuales se debería trabajar, los objetivos buscados y las posibles vías de acción. Interesa destacar la importancia de las políticas de privacidad de los datos, buscando que sean comprensibles y de fácil acceso, siendo importante dar claridad y seguridad, facilitando el acceso y la disponibilidad; así como la protección de los datos de los consumidores y el principio de minimización de datos, limitando la obtención a aquellos que sean necesarios para su funcionamiento. La educación y la sensibilización de los consumidores se presenta como un elemento clave, a fin de que puedan identificar la seguridad de los sistemas y/o dispositivos durante todo el ciclo de vida. Se destaca como buena práctica unir esfuerzos y centralizar la información, coordinando con la colaboración con CERT, a fin de alcanzar respuestas rápidas y poder tomar medidas adecuadas a tiempo.[788]

---

[784] Seguridad en IoT, Proceso en Uruguay, Setiembre 2019. URL: https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/comunicacion/publicaciones/seguridad-iot Consultado el 20 de enero de 2020.
[785] Ibídem, pp. 8.
[786] Ibídem, pp. 9.
[787] Ibídem, pp. 9-11.
[788] Ibídem, pp. 9-12.

Con relación a la resiliencia de la red, se destaca la importancia de proteger la infraestructura de redes ante las potenciales amenazas y vulnerabilidades, buscando formas de mitigar los diversos riesgos identificados, siendo los sistemas y/o dispositivos más expuestos aquellos que están conectados a la red constantemente. Se subraya como fundamental el realizar campañas de sensibilización para aumentar los mecanismos de control, mejorar el diseño y la gestión del ciclo de vida de los sistemas y/o dispositivos, para protegerlos y evitar que sean atacados. En esta línea, se identifican potenciales riesgos, así como posibles vías de mitigación.[789]

Finalmente, se concluye destacando que el número de sistemas y/o dispositivos crece constantemente, siendo esencial promover políticas públicas que favorezcan la concientización de la sociedad en temas de seguridad, así como la participación de todas las partes interesadas para proteger las redes y a los usuarios de manera cabal, impulsando además la investigación, el desarrollo y la difusión.[790]

Por otra parte, se destaca que es fundamental que los diversos actores coordinen acciones y aporten constructivamente para alcanzar soluciones a nivel mundial que contribuyan a proteger a la red y a las personas. [791]

En línea con este último punto, interesa destacar que en el Plan Estratégico de la UIT para los años 2016-2019 se destaca que el fomento de la ciberseguridad, de la cooperación y coordinación internacional es prioridad fundamental, y que la creación de confianza y seguridad ocupa la máxima prioridad en las agendas nacionales, regionales e internacionales[792].

Así, la Resolución 50 de la UIT: "Ciberseguridad" del año 2016, dispone, entre otras cosas, que los aspectos de seguridad se deben tener en cuenta en todos los procesos de elaboración de normas de la UIT,y se encarga un inventario de iniciativas y actividades nacionales, regionales e internacionales dirigidas a fomentar, en la medida que sea posible, la armonización mundial de las estrategias y enfoques adoptados en la materia, así como ayudar a los Estados Miembros en el establecimiento de un marco

[789] Ibídem, pp. 13-16.
[790] Ibídem, pp. 17.
[791] Ibídem, pp. 17.
[792] UIT,Información de referencia sobre el Plan Estratégico de la Unión para 2016-2019. URL: https://www.itu.int/en/council/planning/Documents/Background_Strategic%20Plan%20for%20the%20Union%202016-2019_Spanish.pdf Consultado el 20 de enero de 2020.

adecuado que permita reaccionar rápidamente en caso de incidentes importantes, así como reforzar la protección en dichos países.

(V.3.E) Nuevos desafíos

Como viene de señalarse, Uruguay está siendo muy activo en la materia, desarrollando guías y recomendaciones a fin de atender los desafíos de la temática de la mejor forma.

Sin perjuicio, considerando lo desafiante de la materia aún resta por hacer.

Al respecto interesa destacar que recientemente se publicó el Anteproyecto de Ley de Urgente Consideración, cuyo artículo 214 expresamente prevé el Derecho a la Seguridad digital, estableciendo que *"Los usuarios tienen derecho a la seguridad de las comunicaciones que transmitan y reciban a través de Internet. Los prestadores de servicios de Internet y las entidades públicas informarán a los usuarios de sus derechos y fomentarán la adopción de comportamientos consistentes a al seguridad en Internet"*[793]

Se puede considerar que la seguridad de las comunicaciones en Internet es un derecho inherente a la personalidad humana que deriva del artículo 72 de la Constitución, así como de los artículos 7 y 28 de la Constitución. Además, está en línea con lo establecido en la Ley 18.3331 y en el artículo 11.3 del Reglamento de Licencias de Telecomunicaciones, aprobado por el Decreto 115/003, donde se menciona que los prestadores de servicios deben hacer una declaración jurada por la que se comprometen a adoptar sistemas y procedimientos de seguridad a fin de resguardar la confidencialidad de las comunicaciones que cursen por medio de sus instalaciones y equipos, conforme las reglas del buen arte; así como con la obligación que tienen de garantizar la seguridad de los bienes y de las personas, atendiendo los requisitos en materia de defensa nacional y seguridad pública.

Por otra parte, la obligación de informar los derechos a los usuarios, así como fomentar la adopción de comportamientos consistentes a la seguridad en Internet, se entiende que está en línea con lo establecido en el artículo 6 de la Ley 17.250, específicamente con los derechos de educación y divulgación sobre el consumo

[793] Anteproyecto de Ley de Urgente Consideración, URL: https://lacallepou.uy/anteproyectoLUC.pdf Consultado el 20 de enero de 2020.

adecuados de productos y servicios, además de que también podría considerarse en línea con las medidas dispuestas para la protección de la seguridad.

Finalmente, interesa hacer mención del Convenio sobre la Ciberdelincuencia, aprobado en Budapest en el año 2001, y ratificado por 60 Estados, además de los estados miembros de la Unión Europea, también ha sido ratificado por Estados Unidos, Canadá, Australia, Japón, Israel, República Dominicana, Chile, Argentina, Colombia, Panamá, Costa Rica, Paraguay, entre otros (Convenio de Budapest).

El Convenio de Budapest parte: (i) de los profundos cambios provocados por la digitalización, la convergencia y la globalización; (ii) de la preocupación de que las redes informáticas y la información electrónica sean utilizados para cometer delitos; y (iii) del interés de intensificar la cooperación entre los países, disponiendo la necesidad de aplicar una política penal común con objeto de proteger a la sociedad frente a la ciberdelincuencia, especialmente mediante la adopción de una legislación adecuada y la mejora de la cooperación internacional[794].

En este sentido, el Convenio de Budapest busca armonizar las legislaciones nacionales para enfrentar la ciberdelincuencia y alcanzar una política penal común en la materia para proteger a la sociedad. Para ello establece diversas medidas que deben adoptarse a nivel nacional, comprendiendo aspectos vinculados con el derecho penal sustantivo[795], procesal[796], atendiendo además aspectos de jurisdicción y de cooperación.

Uruguay no ha ratificado el Convenio de Budapest y para poder ser parte debería implementar cambios. En este sentido, es importante evaluar las implicancias del Convenio de Budapest a la luz de la práctica vigente, analizando los aspectos que necesitan mejora en vista de los nuevos desafíos que afrontamos y de la importancia que la cooperación internacional tiene en la materia.

---

[794] Convenio sobre la Ciberdelincuencia, Budapest, 22 de noviembre de 2001. URL: https://www.oas.org/juridico/english/cyb_pry_convenio.pdf Consultado el 20 de enero de 2020.

[795] - Derecho penal sustantivo: (i) delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos; (ii) delitos informáticos; (iii) delitos relacionados con el contenido; (iv) delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines; (v) otras formas de responsabilidad y sanciones.

[796] - Derecho procesal: (i) disposiciones comunes, como ser: ámbito de aplicación de las disposiciones de procedimiento, condiciones y salvaguardias; (ii) conservación rápida de datos informáticos almacenados; (iii) orden de presentación; (iv) registro y confiscación de datos informáticos almacenados; (v) obtención en tiempo real de datos informáticos.

Vale señalar que en el año 2014 el Poder Ejecutivo remitió al Parlamento un proyecto de Ley que pena los delitos informáticos, buscando la conformación de un sistema jurídico que proteja los datos informáticos[797].

En el mismo sentido, en el año 2016 se presentó un proyecto de ley relacionado con disposiciones para combatir la ciberdelincuencia y el uso abusivo de los adelantos tecnológicos. En la exposición de motivos de este segundo proyecto se hace referencia a los objetivos consignados en el Convenio de Budapest, y "*se reconoce la indefectible y urgente necesidad de aplicar una política penal común que proteja a la sociedad frente a la "Ciberdelincuencia" especialmente mediante la adopción de legislaciones adecuadas que conlleven a mejorar la cooperación internacional, asumiendo los cambios ya provocados por la digitalización, convergencia y globalización de las redes informáticas*.[798]"

A la fecha no se ha aprobado una ley específica sobre la materia. Sin perjuicio, vale señalar que como ha destacado el Dr. Martín Pecoy, Uruguay ha tipificado delitos informáticos, específicamente el de falsificación de documento informático (artículo 679 de la Ley 16.736), y el Grooming (artículo 277 bis del Código Penal); mas adolece de una política criminal estructurada en la materia.

(V.4.) Ciberseguridad en España

Se reconoce que garantizar la seguridad en el ciberespacio es un objetivo primordial en las agencias de los Gobiernos, en tanto pueden afectar a la Seguridad Nacional, siendo uno de los mayores desafíos que se debe afrontar[799].

España ratificó el Convenio de Budapest sobre la ciberdelicuencia el 23 de noviembre de 2001, además tiene organismos especializados en la materia y un marco jurídico actualizado.

---

[797] Presidencia de la República Oriental del Uruguay, URL: https://www.presidencia.gub.uy/comunicacion/comunicacionnoticias/seguridad-informatica-proyecto-ley Consultado el 20 de enero de 2020.

[798] Proyecto de Ley presentado por Tabaré Viera. URL: https://parlamento.gub.uy/documentosyleyes/ficha-asunto/103462/ficha_completa Consultado el 20 de enero de 2020.

[799] Ciberseguridad, URL: https://www.dsn.gob.es/es/sistema-seguridad-nacional/qu%C3%A9-es-seguridad-nacional/%C3%A1mbitos-seguridad-nacional/ciberseguridad Consultado el 31 de enero de 2020.

(V.4.A) Ley 36/2015, de 28 de diciembre, de Seguridad Nacional; Real Decreto 12/2018 , de 7 de setiembre, de seguridad de las redes y sistemas de información.

Como surge del preámbulo y del artículo 3 de la Ley 36/2015, *"la Seguridad Nacional se entiende como la acción del Estado dirigida a proteger la libertad y el bienestar de sus ciudadanos, a garantizar la defensa de España y sus principios y valores constitucionales, así como a contribuir junto a nuestros socios y aliados a la seguridad internacional en cumplimiento de los compromisos asumidos; concepto que, hasta la fecha, no había sido objeto de una regulación normativa integral".*

La voluntad es integrar y compartir el fin de la seguridad entre las diferentes Administraciones, el sector privado, la sociedad civil, así como las organizaciones internacionales de las cuales se es parte. La realidad es cada vez más compleja, va más allá de las fronteras de los países, siendo fundamental la transversalidad, siendo esencial la coordinación, para prevenir y responder en todos los niveles y de forma integral.

Se quiere promover a la seguridad como una cultura, con una implicación activa de la sociedad para la preservación y como garantía fundamental para el disfrute de la libertad, la justicia, el bienestar y los derechos de los ciudadanos. A estos fines, se prevé que desde el Gobierno se realizarán acciones y planes para aumentar el conocimiento y la sensibilización de la sociedad acerca de los riesgos y amenazas, así como sobre la necesidad de tomar medidas anticipadas para prevenir, analizar, reaccionar, resistir y recuperar.

Se debe cooperar entre las diversas Comunidades Autónomas, se debe colaborar con el sector privado y promover su participación, y la de todos los ciudadanos, en la formulación y ejecución de la política de Seguridad Nacional.

Entre los ámbitos de especial interés, en tanto son básicos para preservar los derechos y libertades, garantizar el bienestar de los ciudadanos y el suministro de los servicios y recursos esenciales, se encuentran: la ciberseguridad, la seguridad económica y financiera, la seguridad marítima, la seguridad del espacio aéreo y ultraterrestre, la seguridad energética, la seguridad sanitaria y la preservación del medio ambiente[800].

Se celebra el reconocimiento de la importancia que la ciberseguridad, teniendo gran impacto económico y social para todos.

[800] Artículo 10 de la Ley 36/2015.

Hay diversos órganos con competencia en la materia: (a) las Cortes Generales, (b) el Gobierno, (c) el Presidente del Gobierno, (d) los Ministros, (e) el Consejo de Seguridad Nacional, y (f) los Delegados del Gobierno en las Comunidades Autónomas y en las ciudades con Estatutos de Autonomía de Ceuta y Melilla.

Al Consejo de Seguridad Nacional le compete, entre otras cosas, asistir al Presidente del Gobierno en la dirección de la política de Seguridad Nacional y en el Sistema de Seguridad Nacional.

El Sistema de Seguridad Nacional integra al conjunto de órganos, organismos, recursos y procedimientos con competencia en la materia. Le compete *"evaluar los factores y situaciones que puedan afectar a la Seguridad Nacional, recabar y analizar la información que permita tomar las decisiones necesarias para dirigir y coordinar la respuesta ante las situaciones de crisis contempladas en esta ley, detectar las necesidades y proponer las medidas sobre planificación y coordinación con el conjunto de las Administraciones Públicas, con el fin de garantizar la disponibilidad y el correcto funcionamiento de los recursos del Sistema"*[801].

En el 2014 se creó el Consejo Nacional de Ciberseguridad, de apoyo al Consejo de Seguridad Nacional, a fin de coordinar a los organismos con competencia en la materia en el país y desarrollar el Plan Nacional de Ciberseguridad.

La estructura de ciberseguridad en el marco del Sistema de Seguridad Nacional, se constituye de la siguiente forma: (i) el Consejo de Seguridad Nacional, (ii) El Comité de Situación[802], (iii) el Consejo Nacional de Ciberseguridad[803], (iv) la Comisión Permanente de Ciberseguridad[804], (v) el Foro Nacional de Ciberseguridad[805], y (vi) las Autoridades públicas competentes y los CSIRT de referencia nacionales.

[801] Artículo 19 de la ley 36/2015.
[802] Actúa apoyado por el Departamento de Seguridad Nacional, de acuerdo con las directrices político-estratégicas dictadas por el Consejo de Seguridad Nacional en materia de gestión de crisis.
[803] Da apoyo al Consejo de Seguridad Nacional en la dirección y coordinación de la Política de Seguridad Nacional en el ámbito de ciberseguridad.
[804] Es presidida por el Departamento de Seguridad Nacional, facilita la coordinación interministerial a nivel operacional en el ámbito de ciberseguridad. Asiste al Consejo Nacional de Ciberseguridad sobre los aspectos relativos a la valoración técnica y operática de los riesgos y amenazas a la ciberseguridad.
[805] Potencia y crea sinergias público privadas, especialmente para crear conocimiento sobre las oportunidades, desafíos y amenazas a la seguridad en el ciberespacio.

En el 2018 se aprobó el Real Decreto 12/2018, de 7 de setiembre, de seguridad de las redes y sistemas de información, que transpone al ordenamiento jurídico español la Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad en las redes y sistemas de información en la Unión Europea.

Surge de la exposición de motivos que la *"Estrategia de Ciberseguridad Nacional con la que España cuenta desde el año 2013, sienta las prioridades, objetivos y medidas adecuadas para alcanzar y mantener un elevado nivel de seguridad de las redes y sistemas de información. Dicha Estrategia seguirá desarrollando el marco institucional de la ciberseguridad que este real decreto-ley esboza, compuesto por las autoridades públicas competentes y los CSIRT de referencia, por una parte, y la cooperación público-privada, por otra."(...)* Las autoridades competentes vigilarán y sancionarán, promoviendo el desarrollo de las obligaciones establecidas, en consulta con el sector y con las autoridades según corresponda en función de la materia. Por otra parte, *"los CSIRT son los equipos de respuesta a incidentes, que analizan los riesgos y supervisan los incidentes a escala nacional, difunden alertas sobre ellos y aportan soluciones para mitigar sus efectos"*[806].

El Real Decreto reconoce la evolución de las tecnologías y de las comunicaciones, especialmente de Internet, así como el rol fundamental que tienen las redes y los sistemas informáticos para el desarrollo de las actividades sociales y económicas. En este sentido, considerando el impacto, las amenazas, así como los grandes daños que se pueden llegar a generar, es que se regula la seguridad de las redes y sistemas de información utilizados para la provisión de los servicios esenciales y de los servicios digitales[807].

Se entiende por "Redes y Sistemas de información" a: (i) las redes comunicaciones electrónicas, (ii) todo dispositivo o grupo de dispositivos interconectados o relacionados entre sí que realicen tratamiento automático de datos, y (iii) los datos digitales almacenados, tratados, recuperados o transmitidos mediante

[806] Exposición de motivos III, Real Decreto 12/2018, de 7 de setiembre, de seguridad de las redes y sistemas de información.
[807] Real Decreto 12/2018, de 7 de setiembre, de seguridad de las redes y sistemas de información.

redes de comunicaciones electrónicas y/o dispositivos interconectados entre sí que realicen tratamiento automático de los datos[808].

Asimismo, se define "seguridad de las redes y sistemas de información" como la capacidad de resistir toda acción que comprometa la disponibilidad, autenticidad, integridad o confidencialidad de los datos almacenados, transmitido o tratados, o los servicios correspondientes ofrecidos por tales redes y sistemas de información o accesibles a través de ellos[809].

La base es la "*Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, así como todas las recomendaciones y directrices emanadas del grupo de cooperación establecido por el artículo 11 de la citada Directiva, y la información sobre buenas prácticas recopiladas por dicho grupo y la red de CSIRT, regulado en el artículo 12 de aquélla"*[810].

Se prevé que la Estrategia de Ciberseguridad, debe estar alineada con la Estrategia de Seguridad Nacional, estableciendo los objetivos y las medidas para alcanzar un elevado nivel de seguridad de las redes y sistemas de información.

Hay diversas autoridades con competencia en la materia:

para los operadores de servicios esenciales[811]:

---

[808] Artículo 3.A), Real Decreto 12/2018, de 7 de setiembre, de seguridad de las redes y sistemas de información.

[809] Artículo 3.B), Real Decreto 12/2018, de 7 de setiembre, de seguridad de las redes y sistemas de información.

[810] Artículo 4, Real Decreto 12/2018, de 7 de setiembre, de seguridad de las redes y sistemas de información

[811] Definidos en el Artículo 3.D), Real Decreto 12/2018, de 7 de setiembre, de seguridad de las redes y sistemas de información, como: *"entidad pública o privada que se identifique considerando los factores establecidos en el artículo 6 de este real decreto-ley, que preste dichos servicios en alguno de los sectores estratégicos definidos en el anexo de la Ley 8/2011, de 28 de abril."* El artículo 6 del Real Decreto 12/2018 señala que: *"Artículo 6. Identificación de servicios esenciales y de operadores de servicios esenciales.*
1. La identificación de los servicios esenciales y de los operadores que los presten se efectuará por los órganos y procedimientos previstos por la Ley 8/2011, de 28 de abril, y su normativa de desarrollo.
La relación de los servicios esenciales y de los operadores de dichos servicios se actualizará, para cada sector, con una frecuencia bienal, en conjunción con la revisión de los planes estratégicos sectoriales previstos en la Ley 8/2011, de 28 de abril.
Se identificará a un operador como operador de servicios esenciales si un incidente sufrido por el operador puede llegar a tener efectos perturbadores significativos en la prestación del servicio, para lo que se tendrán en cuenta, al menos, los siguientes factores:
a) En relación con la importancia del servicio prestado:

si además son operadores críticos conforme a la Ley 8/2011, de 28 de abril, y si normativo de desarrollo, es la Secretaría de Estado de Seguridad, del Ministerio del Interior, a través del Centro Nacional de Protección de Infraestructuras y Ciberseguridad (CNPIC).

Si no son operadores críticos, es la autoridad sectorial correspondiente por razón de la materia.

para los proveedores de servicios digitales[812], es la Secretaría de Estado para el Avance Digital, del Ministerio de Economía y Empresa.

1.º La disponibilidad de alternativas para mantener un nivel suficiente de prestación del servicio esencial;
2.º La valoración del impacto de un incidente en la provisión del servicio, evaluando la extensión o zonas geográficas que podrían verse afectadas por el incidente; la dependencia de otros sectores estratégicos respecto del servicio esencial ofrecido por la entidad y la repercusión, en términos de grado y duración, del incidente en las actividades económicas y sociales o en la seguridad pública.
b) En relación con los clientes de la entidad evaluada:
1.º El número de usuarios que confían en los servicios prestados por ella;
2.º Su cuota de mercado.
Reglamentariamente podrán añadirse factores específicos del sector para determinar si un incidente podría tener efectos perturbadores significativos.
2. En el caso de tratarse de un operador crítico designado en cumplimiento de la Ley 8/2011, de 28 de abril, bastará con que se constate su dependencia de las redes y sistemas de información para la provisión del servicio esencial de que se trate.
3. En la identificación de los servicios esenciales y de los operadores de servicios esenciales se tendrán en consideración, en la mayor medida posible, las recomendaciones pertinentes que adopte el grupo de cooperación.
4. Cuando un operador de servicios esenciales ofrezca servicios en otros Estados miembros de la Unión Europea, se informará a los puntos de contacto único de dichos Estados sobre la intención de identificarlo como operador de servicios esenciales."

[812] Son proveedores de servicios digitales aquellas personas jurídicas que presten un servicio digital. Servicio digital es un servicio de la sociedad de la información, definido en el Anexo, literal A), de la Ley 34/2002, como: *"todo servicio prestado normalmente a título oneroso, a distancia, por vía electrónica y a petición individual del destinatario.*
El concepto de servicio de la sociedad de la información comprende también los servicios no remunerados por sus destinatarios, en la medida en que constituyan una actividad económica para el prestador de servicios.
Son servicios de la sociedad de la información, entre otros y siempre que representen una actividad económica, los siguientes:
1.º La contratación de bienes o servicios por vía electrónica.
2.º La organización y gestión de subastas por medios electrónicos o de mercados y centros comerciales virtuales.
3.º La gestión de compras en la red por grupos de personas.
4.º El envío de comunicaciones comerciales.
5.º El suministro de información por vía telemática.
No tendrán la consideración de servicios de la sociedad de la información los que no reúnan las características señaladas en el primer párrafo de este apartado y, en particular, los siguientes:

Para los proveedores de servicios esenciales y proveedores de servicios digitales, no siendo operadores críticos y comprendidos en la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector público, es el Ministerio de Defensa, a través del Centro Criptológico Nacional.

Conforme lo establecido en el artículo 10 del Real Decreto 12/2018, de 7 de setiembre, de seguridad de las redes y sistemas de información, a las autoridades competentes, les corresponde:

"a) Supervisar el cumplimiento por parte de los operadores de servicios esenciales y de los proveedores de servicios digitales de las obligaciones que se determinen, conforme a lo establecido en el título VI.

b) Establecer canales de comunicación oportunos con los operadores de servicios esenciales y con los proveedores de servicios digitales que, en su caso, serán desarrollados reglamentariamente.

c) Coordinarse con los CSIRT de referencia a través de los protocolos de actuación que, en su caso, se desarrollarán reglamentariamente.

d) Recibir las notificaciones sobre incidentes que sean presentadas en el marco de este real decreto-ley, a través de los CSIRT de referencia, conforme a lo establecido en el título V.

e) Informar al punto de contacto único sobre las notificaciones de incidentes presentadas en el marco de este real decreto-ley, conforme a lo establecido en el artículo 27.

1.º Los servicios prestados por medio de telefonía vocal, fax o télex.
2.º El intercambio de información por medio de correo electrónico u otro medio de comunicación electrónica equivalente para fines ajenos a la actividad económica de quienes lo utilizan.
3.º Los servicios de radiodifusión televisiva (incluidos los servicios de cuasivídeo a la carta), contemplados en el artículo 3.ª) de la Ley 25/1994, de 12 de julio, por la que se incorpora al ordenamiento jurídico español la Directiva 89/552/CEE, del Consejo, de 3 de octubre, sobre la coordinación de determinadas disposiciones legales, reglamentarias y administrativas de los Estados miembros relativas al ejercicio de actividades de radiodifusión televisiva, o cualquier otra que la sustituya.
4.º Los servicios de radiodifusión sonora, y
5.º El teletexto televisivo y otros servicios equivalentes como las guías electrónicas de programas ofrecidas a través de las plataformas televisivas."

f) Informar, en su caso, al público sobre determinados incidentes, cuando la difusión de dicha información sea necesaria para evitar un incidente o gestionar uno que ya se haya producido, conforme a lo establecido en el artículo 26.

g) Cooperar, en el ámbito de aplicación de este real decreto-ley, con las autoridades competentes en materia de protección de datos de carácter personal, seguridad pública, seguridad ciudadana y seguridad nacional, así como con las autoridades sectoriales correspondientes, conforme a lo establecido en los artículos 14 y 29.

h) Establecer obligaciones específicas para garantizar la seguridad de las redes y sistemas de información y sobre notificación de incidentes, y dictar instrucciones técnicas y guías orientativas para detallar el contenido de dichas obligaciones, conforme a lo establecido en los artículos 16 y 19.

i) Ejercer la potestad sancionadora en los casos previstos en el presente real decreto-ley, conforme a lo establecido en el título VII.

j) Promover el uso de normas y especificaciones técnicas, de acuerdo con lo establecido en el artículo 17.

k) Cooperar con las autoridades competentes de otros Estados miembros de la Unión Europea en la identificación de operadores de servicios esenciales entre entidades que ofrezcan dichos servicios en varios Estados miembros.

l) Informar al punto de contacto único sobre incidentes que puedan afectar a otros Estados miembros, en los términos previstos en el artículo 25."

Respecto a la supervisión de los operadores de servicios esenciales: las autoridades les podrán requerir toda la información necesaria para evaluar la seguridad de las redes y sistemas de información, incluida la documentación sobre políticas de seguridad, así como la aplicación efectiva de la política, y auditar o exigir que se sometan a auditorias por una entidad externa, solvente e independiente. En función de ello, se le podrá requerir que subsane las deficiencias detectadas e indicarle cómo debe hacerlo[813].

[813] Artículo 32 del Real Decreto 12/2018, de 7 de setiembre, de seguridad de las redes y sistemas de información

En el caso de la supervisión de los proveedores de servicios digitales, las autoridades competentes solo podrán inspeccionar el cumplimiento cuando tengan noticia de algún incumplimiento o cuando tenga petición razonada por otros órganos o denuncia[814].

Cuando corresponda, la supervisión se hará en cooperación con las autoridades competentes de los Estados miembros en los que se ubiquen las redes y sistemas de información empleados para la prestación del servicio, o en donde esté establecido el operador del servicio, o en donde esté establecido el operador de servicios esenciales, el proveedor de servicios digitales o su representante[815].

Se prevén equipos de respuesta a incidentes de seguridad informática (CSIRT) para las relaciones son los operadores de servicios esenciales (el Centro Criptológico nacional -CCN-CERT-, el Instituto Nacional de Ciberseguridad de España -INCIBE-CERT-, y el Ministerio de Defensa – ESPDEF-CERT), y para las relaciones con los proveedores de servicios digitales que no estuvieran comprendidos como esenciales. Para los ciudadanos, entidades de derecho privado y otras entidades, el INCIBE- CERT es el equipo de respuesta.

Los CSIRT se deben coordinar entre sí y con el resto de los CSIRT nacionales e internacionales.

El Centro Criptológico Nacional (CCN) ejerce la coordinación nacional de CSIRT en materia de seguridad de las redes y sistemas de información del sector público[816], y es el enlace para garantizar la cooperación transfronteriza de los CSIRT de las Administraciones Públicas, para responder a los incidentes y gestionar los riesgos de seguridad. A su vez, los CSIRT de las Administraciones públicas deben consultar y colaborar, cuando corresponda, con los órganos en materia de seguridad nacional, seguridad pública, seguridad ciudadana y protección de datos de carácter personal.

Por otra parte, el título V del Real Decreto 12/2018, de 7 de setiembre, de seguridad de las redes y sistemas de información, prevé la obligación de notificar los

[814] Artículo 33 del Real Decreto 12/2018, de 7 de setiembre, de seguridad de las redes y sistemas de información

[815] Artículo 34 del Real Decreto 12/2018, de 7 de setiembre, de seguridad de las redes y sistemas de información

[816] comprendido en la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, y en la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

incidentes. En este sentido, se dispone la obligación de los proveedores de servicios esenciales y de los proveedores de servicios digitales, de notificar de los incidentes que puedan tener efectos perturbadores en los servicios. En el caso de los proveedores de servicios esenciales, deben notificar los eventos que puedan tener efectos perturbadores, así como aquellos que aún no hayan tenido efecto adverso. En cambio, los proveedores de servicios digitales, deben notificar los incidentes que tengan efectos perturbadores significativos y cuando tenga acceso a la información necesaria para valorar el impacto del incidente.

Para determinar la importancia de los efectos de un incidente, se consideran como mínimo los siguientes factores: el número de usuarios afectados, la duración del incidente, la extensión o áreas geográficas afectadas por el incidente, el grado de perturbación del funcionamiento del servicio, el alcance del impacto en actividades económicas y sociales cruciales, la importancia de los sistemas afectados o de la información afectada por el incidente para la prestación del servicio esencial, y el daño a la reputación[817].

Los operadores de servicios esenciales y los proveedores de servicios digitales están obligados a[818]:

resolver los incidentes de seguridad que les afecten,

solicitar ayuda especializada, incluida la del CSIRT de referencia, cuando no puedan resolver por sí mismos los incidentes.

atender las indicaciones que reciban del CSIRT para resolver el incidente, mitigar sus efectos y reponer los sistemas afectados.

suministrar al CSIRT de referencia y a la autoridad competente toda la información que se les requiera para el desempeño de sus funciones.

Interesa destacar que las autoridades competentes y los CSIRT de referencia deben cooperar y comunicar, sin dilación, a la Agencia Española de Protección de Datos

[817] Artículo 21 del Real Decreto 12/2018, de 7 de setiembre, de seguridad de las redes y sistemas de información

[818] Artículo 28 del Real Decreto 12/2018, de 7 de setiembre, de seguridad de las redes y sistemas de información

para hacer frente a los incidentes que den lugar a violaciones de datos personales, y la mantendrán informada sobre la evolución de tales incidentes[819].

En definitiva, el interés nacional requiere de mayor coordinación, buscado la prevención y responder debidamente, organizándolo de manera integral,

(V.4.B) Estrategia de Ciberseguridad

En diciembre de 2013 España aprobó la primer Estrategia de Ciberseguridad por el Consejo de Seguridad Nacional, partiendo de la necesidad de una acción sincronizada y coordinada de todos los recursos del Estado, haciendo partícipes a todos, sector privado, ciudadanos, sociedad civil, teniendo en cuenta a la Unión Europea, organizaciones nacionales e internacionales, así como los países del entorno[820].

En abril de 2019 el Consejo de Seguridad Nacional aprobó una actualización de la Estrategia Nacional de Ciberseguridad. Parte de la base de que la ciberseguridad va más allá de la protección del patrimonio tecnológico, adentrando en las esferas políticas, económicas y sociales. Siendo clave la colaboración público-privada, así como una nueva aproximación.

Va en línea con la Estrategia de Seguridad Nacional de 2017, amplía el objetivo para la ciberseguridad, para garantizar el uso seguro y fiable del ciberespacio, proteger los derechos y las libertades, y promover el desarrollo económico y social[821].

El fin de la Estrategia Nacional de Ciberseguridad de 2019 es fijar las directrices generales y se basa en los principios de la Seguridad Nacional: unidad de acción, anticipación, eficiencia y resiliencia[822].

La unidad de acción: busca la coordinación entre los distintos agentes, a fin de ser coherentes, resolver de manera rápida, eficaz e integral.

La anticipación: apunta a las actuaciones preventivas, requiere de organismos especializaciones que puedan orientar en casos de crisis, tanto a nivel del Estado como

---

[819] Artículo 29 del Real Decreto 12/2018, de 7 de setiembre, de seguridad de las redes y sistemas de información

[820] Ciberseguridad, URL: https://www.dsn.gob.es/es/sistema-seguridad-nacional/qu%C3%A9-es-seguridad-nacional/%C3%A1mbitos-seguridad-nacional/ciberseguridad

[821] Estrategia Nacional de Ciberseguridad, Gobierno de España, julio 2019, URL: https://www.dsn.gob.es/es/documento/estrategia-nacional-ciberseguridad-2019 Consultado el 31 de enero de 2020.

[822] Estrategia Nacional de Ciberseguridad, Gobierno de España, julio 2019, URL: https://www.dsn.gob.es/es/documento/estrategia-nacional-ciberseguridad-2019 Consultado el 31 de enero de 2020.

en el sector privado. Así como disponer de sistemas eficaces, con información compartida para poder responder en tiempo real.

La eficiencia: considera que la ciberseguridad exige un alto nivel tecnológico, con necesidades exigentes y alto coste derivado de su desarrollo, adquisición y operación, por lo que se debe orientar la acción hacia la optimización y la eficiencia.

La resiliencia: es una particularidad que tienen que tener los sistemas e infraestructuras críticas, en especial las redes de información y comunicaciones frente a las ciberamenazas.

En línea con lo anterior, se establecen cinco objetivos.

El primero: consolidar un marco nacional coherente e integrado para la seguridad y resiliencia de las redes y los sistemas de información y comunicaciones del sector público y de los servicios esenciales. Para lo cual se prevén medidas para mejorar la prevención, detección y respuesta ante incidentes, desarrollando soluciones y reforzando la coordinación.

El segundo: garantizar el uso seguro y fiable del ciberespacio frente a usos ilícitos o maliciosos. Se identifican tres ámbitos de lucha contra la cibercriminalidad en el ciberespacio: (i) como objetivo directo de los hechos delictivos, (ii) como medio clave para su comisión, y (iii) como medio u objeto directo de investigación de un hecho ilícito. Previendo la necesidad de una regulación sólida y eficaz, así como el fortalecimiento de la cooperación judicial y policial, a nivel nacional e internacional.

El tercero: proteger el ecosistema empresarial y social y de los ciudadanos. Se reconoce que las personas y organizaciones tienen derecho a hacer un uso seguro del ciberespacio, y la responsabilidad del Estado de promover e impulsar las medidas necesarias para mantener un nivel suficiente de ciberseguridad, así como de proteger a los más vulnerables y permitir el desarrollo socioeconómico.

El cuarto: crear cultura y compromiso con la ciberseguridad y potenciar las capacidades humanas y tecnológicas. Se necesita recursos técnicos y humanos que proporcionen la capacidad adecuada para el uso seguro del ciberespacio y el desarrollo de actividades de investigación, desarrollo e innovación en ciberseguridad, fomentando el uso de productos y servicios certificados.

El quinto: promover la seguridad del ciberespacio en el ámbito internacional. En este ámbito, se busca un ciberespacio abierto, plural, seguro y confiable, para lo cual se trabajará para crear un marco internacional para prevenir conflictos, cooperar y dar estabilidad en el ciberespacio. Se reconoce la importancia del multilateralismo, así como el rol de las Naciones Unidas para construir consensos que fomenten la confianza, la colaboración y la participación.

En vista de los objetivos señalados se establecen las siguientes líneas de acción[823]:

Reforzar las capacidades ante las amenazas provenientes del ciberespacio.

Garantizar la seguridad y resiliencia de los activos estratégicos.

Reforzar las capacidades de investigación y persecución de la cibercriminalidad, para garantizar la seguridad ciudadana y la protección de los derechos y libertades en el ciberespacio.

Impulsar la ciberseguridad de ciudadanos y empresas.

Potenciar la industria de ciberseguridad, la generación y retención de talento, para el fortalecimiento de la autonomía digital.

Contribuir a la seguridad del ciberespacio en el ámbito internacional, promoviendo un ciberespacio abierto, plural, seguro y confiable, en apoyo de los intereses nacionales.

Desarrollar una cultura de ciberseguridad.

Se reconoce que las amenazas y los desafíos evolucionan de forma continua. Es necesaria una rápida adaptación del ecosistema, así como una gobernanza madura, donde deben participar todos los sectores de la sociedad. En esta línea, se prevé que la estrategia debe adaptarse y revisarse continuamente.

Finalmente, como ya se mencionó, al hacer referencia a la protección de los DP en España y el Impacto del RGPD, con la Ley Nº 3/2018 no solo ha transpuesto el RGPD en la regulación nacional, sino que además ha ido más allá, reconociendo expresamente los nuevos derechos que derivan de la era digital. Ente los nuevos derechos, en el artículo 82 se estableció que " *Los usuarios tienen derecho a la seguridad de las*

[823] Estrategia Nacional de Ciberseguridad, Gobierno de España, julio 2019, URL: https://www.dsn.gob.es/es/documento/estrategia-nacional-ciberseguridad-2019 Consultado el 31 de enero de 2020.

comunicaciones que transmitan y reciban a través de Internet. Los proveedores de servicios de Internet informarán a los usuarios de sus derechos."

Asimismo, el artículo 83 de la Ley Nº 3/2018, en relación al derecho a la educación digital, se prevé que "*Los planes de estudio de los títulos universitarios, en especial, aquellos que habiliten para el desempeño profesional en la formación del alumnado, garantizarán la formación en el uso y seguridad de los medios digitales y en la garantía de los derechos fundamentales en Internet."*

En la Disposición adicional novena de la Ley Nº 3/2018, en relación con la notificación de incidentes de seguridad, prevé que "*cuando deban notificarse incidentes de seguridad, las autoridades públicas competentes, equipos de respuesta a emergencias informáticas (CERT), equipos de respuesta a incidentes de seguridad informática (CSIRT), proveedores de redes y servicios de comunicaciones electrónicas y proveedores de tecnologías y servicios de seguridad, podrán tratar los datos personales contenidos en tales notificaciones, exclusivamente durante el tiempo y alcance necesarios para su análisis, detección, protección y respuesta ante incidentes y adoptando las medidas de seguridad adecuadas y proporcionadas al nivel de riesgo determinado*".

El 17 de abril de 2019 el Parlamento Europeo y del Consejo aprueba el Reglamento (UE) 2019/881 relativo a ENISA (Agencia de la Unión Europea de la Ciberseguridad) y a la certificación de la ciberseguridad de las tecnologías de la información y la comunicación y por el que se deroga el Reglamento (UE) 526/2013.

El objeto del Reglamento es alcanzar un nivel elevado de ciberseguridad, ciberresiliencia y confianza dentro de la Unión, para lo cual se establecen los objetivos, tareas y aspectos organizativos relativos a ENISA, así como un marco para la creación de esquemas europeos de certificación de la ciberseguridad, a efectos de garantizar un nivel adecuado de ciberseguridad de los productos, servicios y procesos de TIC en la Unión.

Define "ciberseguridad" como *"todas las actividades necesarias para la protección de las redes y sistemas de información, de los usuarios de tales sistemas y de otras personas afectadas por las ciberamenazas*", y "ciberamenazas" como "*cualquier situación potencial, hecho o acción que pueda dañar, perturbar o afectar*

desfavorablemente de otra manera las redes y los sistemas de información, a los usuarios de tales sistemas y a otras personas"[824].

Además, según se difundió, el 17 de mayo de 2019 el Consejo ha establecido un marco que permite a la UE imponer medidas restrictivas específicas para impedir y responder a los ciberataques que sean una amenaza para la UE o sus Estados miembros[825]. Además el 3 de diciembre de 2019, se han difundido Conclusiones del Consejo sobre la tecnología 5G, los riesgos que puede implicar y las medidas que serán necesarias para poder mitigar los riesgos y garantizar la seguridad[826].

(V.5.) Consideraciones finales

La seguridad en la era digital cobra cada vez más trascendencia, en tanto impacta a todos (ciudadanos, empresas, gobiernos, etc.), en todo (sistemas, dispositivos, cosas, servicios, etc.), y crece de forma constante, teniendo la potencialidad de generar grandes daños.

La digitalización, la gran penetración de internet, la interconexión que facilita, y el desarrollo de aplicaciones digitales, son muy beneficiosos para todos dado que, entre otras cosas, borran fronteras y son un trampolín a nuevos derechos y libertades. Sin perjuicio, como contrapartida, nos exponen a nuevos y constantes riesgos sobre los cuales necesariamente debemos trabajar a fin de mitigar.

En este sentido, considerando la velocidad de los cambios, generar guías que sirvan de base, así como tener en cuenta los principios fundamentales, parece primordial. Se destaca la importancia de:

Tomar conciencia, ser responsables del rol que cada uno tiene, y responder debidamente, respetando los principios democráticos.

Evaluar los riesgos, identificar las amenazas y las vulnerabilidades a fin de mitigarlas.

---

[824] Artículo 2 del Reglamento (UE) 2019/881.

[825] Consejo de la Unión Europea, URL: https://www.consilium.europa.eu/es/press/press-releases/2019/05/17/cyber-attacks-council-is-now-able-to-impose-sanctions/ Consultado el 31 de enero de 2020.

[826] Council of the European Union, Council Conclusions on the significance of 5G to the European Economy and the need to mitigate security risks linked to 5G. URL: https://www.consilium.europa.eu/media/41595/st14517-en19.pdf Consultado el 31 de enero de 2020.

Diseñar, ejecutar, coordinar y actuar rápido, para garantizar la seguridad de la información, de los productos, servicios, sistemas y redes.

Gestionar debidamente la seguridad, prevenir, detectar, y reevaluar las medidas adoptadas.

Cooperar y coordinar a nivel nacional e internacional entre los diversos actores, compartiendo información y acciones, aunando esfuerzos para la lucha contra el cibercrimen.

Pero además, como se estableció en España es fundamental: reforzar las capacidades ante las amenazas que provienen del ciberespacio, garantizar la resiliencia de los activos estratégicos, reforzar las capacidades de investigación, impulsar la ciberseguridad de ciudadanos y empresas, potenciar la industria de ciberseguridad, así como la generación y retención de talentos, contribuir a nivel internacional, y desarrollar una cultura de ciberseguridad.

Uruguay ha venido trabajando y haciendo esfuerzos por prevenir, concientizar y cumplir con los estándares internacionales. Se busca dar seguridad tanto a las personas, físicas y jurídicas, como a las cosas; generando instancias de trabajo conjunto entre los diversos actores involucrados, atendiendo las mejores prácticas internacionales.

Sin embargo, la materia presenta múltiples desafíos de evolución constante, siendo la cooperación y coordinación internacional cada vez de mayor relevancia. En esta línea, parece fundamental analizar y tomar las medidas que la realidad y los desafíos actuales requieren, así como agilizar y profundizar los trabajos en esta área, considerando los instrumentos internacionales existentes, a fin de dar garantías, confianza y seguridad a todos.

España presenta un arco y un trabajo bastante más avanzado y desarrollado. No solo ratificó el Convenio de Budapest sobre la ciberdelincuencia el 23 de noviembre de 2001, sino que además tiene organismos especializados en la materia y un marco jurídico actualizado. También tiene previstos los objetivos, los lineamientos y la estructura de actuación, y va más allá haciendo énfasis en los derechos de los usuarios y en la importancia de la educación.

Se considera de muy buena práctica el trabajo que está realizando España, en tanto procura integrar y compartir el fin de la seguridad entre las diferentes Administraciones, el sector privado, la sociedad civil, así como las organizaciones

internacionales de las cuales se es parte. Entienden que la realidad es cada vez más compleja, que va más allá de las fronteras de los países, siendo fundamental la transversalidad y la coordinación, para prevenir y responder adecuadamente en todos los niveles y de forma integral.

Sin embargo, como reconocen, la materia es de evolución constante por lo que es esencial la reevaluación, revisando y modificando lo que sea necesario para poder responder debidamente a los nuevos desafíos y amenazas. Así como tomar acciones proactivamente para generar una cultura en ciberseguridad.

CONCLUSIONS

We are in a time of great economic and social changes, which impact everything, everyone and at exponential speeds.

Digitalization plays a key role, generating multiple opportunities and challenges that impose on the legal system the challenge of adapting and responding adequately to the new context.

The digital revolution and the transformation that it entails, is a process that has been evolving and integrating, thanks to the development telecommunications has had, the platforms and the diverse technologies; and that, thanks to the globalization, has been universalized, being more and more affordable and accessible.

Nevertheless, there is still much to be done. It is essential to take steps to narrow the digital division and connect everyone, while protecting people's fundamental rights - such as their security, privacy, equality and freedom of speech - and promoting competition, innovation and development.

Therefore, we are obliged to develop solutions to protect and promote Human Rights to ensure their effectiveness, as they are essential to achieve freedom, justice and peace, being fundamental, as it arises from the Universal Declaration of Human Rights, teaching and education, respect for these rights and freedoms, as well as the adoption of national and international measures for their recognition and implementation.

I welcome the fact that the development of connectivity and technology has facilitated the creation and universalization of new digital services and applications, which respond to various social and economic needs, which are provided on electronic platforms, and which have generated a digital ecosystem that erases borders, reflects that we live in an international community, offers more access, empowers people and generates multiple opportunities.

I applaud the fact that the digital ecosystem facilitates innovation and solutions that make life easier for everyone, with a positive impact on society. However, we cannot ignore the fact that a misuse of tools can affect the general interest, as well as violate Human Rights.

In this environment, as recognized by the World Summit on the Information Society in 2015, among the main challenges on which we must work, I highlight the following:

- Protect all Human Rights, ensuring that they are respected both online and offline.

- Integrate the equality perspective, seeking to empower women, their full participation, as well as equality in all spheres of society and in decision-making processes.

- Reduce the digital division. Expand access to Information and Communication Technologies (ICTs) and connect everyone, for which it is necessary to improve the management and use of the radioelectric spectrum, as well as facilitate the construction and implementation of telecommunications networks.

- Increase access to information, education and knowledge for all. It is necessary that all people have the basic knowledge to participate in the information society.

- To guarantee the full right of all people to express themselves, to create and to disseminate their works and contents.

- Respecting human diversity in all its forms, culture, languages, traditions, beliefs and religions.

- Generate confidence in the use of ICT, being essential to increase security and privacy on the network.

- Raise awareness of the ethical dimension of the use of ICTs and encourage interdisciplinary dialogue.

The challenges and objectives are many, but the essential aspect is to identify and work on them, together with the various actors in society, so that the Internet and the digital ecosystem can continue developing, in a safe and inclusive environment that promotes innovation, development and research, while ensuring the fundamental rights of all.

In this sense, it is not only important to be agile and to act with transparency, as well as to collaborate with each other, but it is also fundamental that we work on education and give security to people so that they trust, adopt the changes and be part of these changes.

Having said that, I would like to emphasize the importance of analyzing the new reality in its entirety and highlight the role of the regulator to achieve balance, as well as the need to tend to a collaborative regulation, suitable, necessary and weighted in light of the objectives.

We must learn from the experiences of others. We do not have to invent the wheel every time.

The new digital reality not only offers endless opportunities and benefits for society, but also presents multiple challenges that societies must face acting together.

Digital agendas - both at a regional and country level - are a clear guide and tool for working on this issue, since they show the several elements of the ecosystem that need to be developed in order to achieve the digital transformation in the best way.

In this context, the law, regulators, as well as public policy makers, face many challenges as a tool to ensure that the rights that individuals and companies have in the offline or traditional world are also held in the *online* or digital world. At the same time, in such a changing scenario, where profound economic and social modifications are generated in a vertiginous way, the fundamental principles take on increasing relevance; it is essential to analyze and address the new reality in its globality. We cannot respond adequately to it, pretending that it adjusts to regulations or to situations designed for completely different assumptions.

The change is continuous, it is cardinal to understand the technical and business aspects, as well as the collaborative work and constant dialogue between the various parties. Flexibility and adaptability are basic, it is necessary to review the current regulations and those that are dictated, in addition it is essential to review with humility since it can be that the current no longer reflects the reality, at the time that it is not necessary nor proportional.

Before regulating, it is paramount to identify what you want to regulate, what is the risk or problem you want to address, or what are the sustainability, efficiency or equity aspects that require attention. Likewise, it is necessary to observe if the proposed measures are proportional, suitable and mandatory for the purpose sought.

Regulation must be an element that contributes to innovation and development, that provides predictability and that allows to attract investments; for which, it is crucial

that it is developed in a collaborative way with the market, giving security, transparency and clear rules.

The digital revolution poses multiple opportunities and challenges that we must necessarily address, this new reality impacts everyone and everything, at great speed, and allows to accelerate the achievement of the Sustainable Development Goals, approved by the United Nations for 2030. But without a doubt, the above requires various actions that must be coordinated, controlled and adjusted, at the national, regional and international levels, in order to fully comply with the goals sought.

Telecommunication networks, mainly Internet connectivity, together with the great development of technologies, are a fundamental part in the digital transformation, as they are the backbone on which the entire digital ecosystem is developed.

In the face of so much information and so many changes, all of which occur at exponential speed; being clear, acting with agility and in a collaborative manner, is essential. Law and Regulation play a key role in providing security, transparency and predictability. Poor regulation, either because it is excessive or because it is not in line with reality, can greatly affect society, as it can limit innovation, development, research and discourage investment.

With the development of technologies and digital convergence, the ecosystem has been transformed, with multiple benefits for users, while competition increases, allowing people to access more services, at lower prices.

We see the effects of convergence in the networks, in the way services are provided, in the devices we use, as well as in the great variety of content we can share and access.

Borders are being erased and the way services are provided is constantly evolving, they can be provided by various means, and it is essential that the service is attended to and that the principle of technological neutrality is recognized, as well as the efficient sharing of resources, such as the radio spectrum, physical space, network support and access and transport networks.

The assumptions must be analyzed thoroughly, looking for the answers in the general principles, leaving without effect what is no longer necessary, updating what is required and putting people at the center, as well as the social and economic development of all.

The global nature of the Internet and the speed of change mean that international coordination, the *multistakeholder* model and self-regulation are becoming increasingly important.

There is also a growing need to simplify and harmonize, to provide predictability and security, in order to promote innovation and development.

The following are of great relevance: (i) the need for regulators to be independent, acting in an impartial, objective, transparent, non-discriminatory and proportionate manner; (ii) infrastructure sharing and appropriate resource management, such as harmonization and coordination in the use of the radio spectrum and numbering; and (iii) coordination, dialogue and exchange at the national, regional and international levels.

With digitalization come major economic and social changes, which imply great benefits for people, while generating risks for fundamental rights and for the traditional economy if adequate measures are not taken and regulations are not adjusted. It is necessary to ensure that fundamental rights are respected, that competitive advantages are not generated as a result of regulatory asymmetries, and that the same services, regardless of the medium through which they are provided, have the same regulations.

The way is not to prohibit or establish meaningless regulations; we have to rethink the models. Innovation must be welcomed and promoted, and it is essential that specialists from different disciplines work together, as well as that there is proper coordination among the various actors in the sector, at the international, regional and national levels. We must rely on general principles, *multistakeholder* models and self-regulation.

In Uruguay, in order to provide telecommunications services, administrative acts, issued by the Executive Branch, are required to be expressly authorized. We are dealing with private activity, of public interest, which is governed by the principle of free and healthy competition, except for the exceptions provided by law.

In Spain, authorizations do not have to be express and are not per type of service, and one of the main cases identified for the ICT Revolution was precisely the liberalization of telecommunications and the economic benefits it brings.

The authorizations and/or licenses are by classes of services in Uruguay, in addition the administrative acts provide the scope, requirements and conditions, as well

as the rights and obligations arising from them. In Spain the regime has already evolved, not differentiating by classes of services, and actually applying the principle of technological neutrality.

Considering -among other things-: (i) the convergence, (ii) the change that has been generated in the traditional models with the digital transformation, (iii) the great development of the advanced technologies, (iv) that now practically everything goes through the Internet, (v) that the competition is every time greater and not only among companies of the same segment, (vi) that the client is indifferent to the means through which the final service is provided, (vii) that more investments are needed in last generation telecommunications networks, being fundamental the effective and efficient use of the resources; the trend is towards a single telecommunications license -which enables the provision of all telecommunications services, fixed or mobile, wired or wireless, with or without its own infrastructure-, and the sharing of infrastructure and radio-electric spectrum.

In order for the digital transformation to develop properly, the deployment of state-of-the-art networks is essential. This requires, among other things: providing security, clear rules, predictability, meeting the principle of technological neutrality, convergence and sharing of resources, as well as making the necessary regulatory adjustments and updates.

The radio spectrum is a natural, intangible, shared, limited, scarce resource, which is divided into frequency bands, through which the electromagnetic waves of wireless communication services are transmitted.

It is part of the public domain of the States, who administer, manage and control it at the national level; but the ITU, as well as other regional bodies have a fundamental role in the management, coordination, harmonization at the global level.

It is in high demand and is essential for the digital transformation, for connectivity, for access, for the development of wireless, mobile and fixed services, as well as for the deployment of last generation networks; which is essential to diminish the digital gap, facilitate innovation, promote education, universalize new technologies and develop the digital economy.

In this context, the availability of spectrum, the principle of technological and service neutrality, as well as the coordination and sharing of resources among the

various actors take on greater relevance; it is essential to provide security, clear rules, and predictability, in order to attract investment and promote deployment, making the necessary regulatory adjustments and updates.

The existing regulation in Spain, unlike that of Uruguay, seems to reflect to a great extent the new digital reality. Regulation in Uruguay should be analyzed and updated in order to facilitate development and innovation. The model followed in Spain could be a good guide for Uruguay.

The digital services and applications provided through platforms have generated a new economy, which has many benefits, while presenting multiple challenges.

The subject is extremely up-to-date, both regionally and nationally, is working and analyzing how to face this new reality, seeking the development of the digital economy and the protection of fundamental rights of individuals, while promoting innovation and investment, controlling risks, protecting competition, consumers and users.

Digital platforms offer a world of opportunities and benefits for users; without a doubt it is necessary to identify the risks and work on them to mitigate them, but innovation is essential for economic and social development.

The dialogue between the different actors is fundamental, the changes are occurring more and more quickly and the regulation plays a very important role, being basic that it is adequate, that it is revised and updated if necessary, so that it attends the reality of the sector, that it does not limit it without real arguments, at the same time that it protects the users and grants legal security to facilitate the innovation, the development and to attract investments.

A good practice that is being implemented in comparative law is the "*sandbox*" method, which allows real trials between companies and regulators, in controlled environments, for a given period of time. They generate an ecosystem similar to the real market, where companies, regulators and consumers interact, learn together, and identify the points and guarantees that need to be addressed.

We cannot pretend to respond adequately to the new realities, with models and solutions designed for different scenarios. We have to reach more innovative and efficient solutions, which allow us to develop and create jobs, attract talent and investments.

We must empower people, protect them, and promote the development of networks and digital services and applications, seeking to make them accessible to all. Promoting innovation and defending competition is fundamental, as well as leaving behind the regulation of rigid preconceived frameworks, to start working in the new dynamic reality of permanent change.

ICTs cut across all sectors of the economy and as such regulation must acquire a collaborative character, with articulation between the various actors being fundamental. Clear rules are needed, which should not be confused with rigid regulations that quickly become outdated and end up limiting. We must provide frameworks that promote and encourage, providing security without limiting.

Regulation is a factor that will facilitate and differentiate countries. Those who understand, attend to and promote the new reality, with a comprehensive vision, will better develop the ecosystem, generating more opportunities for all.

It is essential to respond in a more intelligent, adequate manner, avoiding errors, attending to the need and reality, in a proportional manner.

For which we must: (i) Learn from the experiences that other countries already have, some of which have more experience in this area. (ii) Work together, understand and dialogue among the various actors in the sector. (iii) Measure, control and periodically review the solutions adopted.

Spain's legal framework has been developing and updating for more than fifteen years. In Uruguay there are bills on the subject and regulations of various rankings, but in many cases they do not reflect current events and needs.

The Spanish regulation on FINTECH was criticized for not adapting to reality and needs, which led many companies to set up in more friendly countries with clearer rules, such as England. Uruguay should learn from Spain's experience, both from the positive and negative aspects.

The regulation must be more intelligent, flexible, carried out together, being fundamental the periodic review in order not to affect innovation, development, research and investment. The changes are happening very fast and the countries that better respond to the new digital reality will generate more opportunities for their citizens.

The Internet and new technologies have facilitated the creation of new digital services and applications, which have generated a digital ecosystem that erases borders, reflects that we live in an international community, offers more access, empowers people and generates multiple opportunities.

It is essential, among other things: (i) empowering people, (ii) ensuring equality, (iii) reducing the digital divide, (iv) increasing education, knowledge and access to information, (v) ensuring free expression, (vi) increasing security and privacy, (vii) building trust, and (viii) promoting interdisciplinary dialogue, with a focus on working together among the various actors in the ecosystem, at the national, regional and international levels.

With Law No. 3/2018, Spain has not only transposed the GDPR into national regulations, but has also gone further, expressly recognizing the new rights that derive from the digital era.

Uruguay, with articles 72 and 332 of the Constitution, has the possibility of considering that these rights have a constitutional backing and protection, insofar as they can be considered as rights inherent to the human personality, not being necessary their express consecration in order to be recognized.

Without prejudice, I consider that the direct recognition, as it was done in Spain, is a good practice insofar as it facilitates the universalization, protection and the effectiveness of the same.

Artificial intelligence, robotics and the ability of machines to learn by themselves, generate multiple questions related to intellectual property, which are essential to analyze and respond in order to provide certainty, security and support for innovation.

Security in the digital era is becoming increasingly important, as cybercrimes impact everyone (citizens, companies, governments, etc.), and everything (systems, devices, things, services, etc.), and are growing constantly, with the potential to generate great damage. This is one of the great challenges at both the national and global levels, as they have the potential to attack from anywhere in the world, generating a global impact. In this line, it is important to prohibit the various types of cyber-attacks that can be carried out, that individuals, companies and governments implement preventive and proactive protection measures, following good practices, which are constantly updated and knowledge is shared.

In this regard I believe it is important to: (i) generate a safety culture of protection and prevention; (ii) increase awareness of cyber-risk and the importance of prevention; (iii) promote greater trust, where education is essential; (iv) create frameworks that facilitate the understanding and adoption of the various security measures available; (v) cooperate and exchange information; and to (vi) promote knowledge in this field.

Digitalization, the great penetration of the internet and interconnection, facilitates the development of new services and digital applications that are very beneficial to all, since, among other things, it empowers people, gives them more freedom and a greater scope in the enjoyment of their rights, and is a springboard for new rights and freedoms. However, in turn, it exposes us to new and constant risks that we must necessarily work to mitigate.

The Spanish legal system is more up-to-date and responds to the new legal challenges that digitalization brings with it in a more appropriate way than the Uruguayan system. However, it has aspects to work on, not only because everything is evolving very fast, changes are constant, and new challenges and vulnerabilities are being identified - as for example in content moderation and the effect this can have on freedom of expression and access to information, or for example what happens to the intellectual property of robots - but also because there are already specific aspects that have been highly criticized by the industry, such as the lack of clear rules in the Fintech sector. Uruguay's regime is far more backward and outdated than Spain's. Some solutions no longer meet the needs or adapt to reality, but it is worth noting that changes have begun to be made, such as strengthening and giving more independence to the regulator.

Uruguay's legal framework is far more backward than the Spanish one. In many cases there are no clear rules and in others the solutions are no longer adapted to the markets, for example for some companies it is forbidden to provide data and television services together, which is clearly contrary to technological convergence. In addition, it is worth noting that in fact there is still a monopoly in the provision of fixed data, at the moment it is proposed that new operators will begin to operate, but there is no specific regulation or clear rules on aspects that may be important for implementation.

In this sense, we emphasize that the revision and updating of the solutions must be constant, simple, clear, flexible, necessary, suitable, and meet reality.

Finally, considering the speed of change and the global impact that digitization entails, I believe it is very convenient to learn from the good and bad experiences of other countries, to create regulatory sandboxes, as well as to generate guidelines that serve as a basis, taking into account the fundamental principles and promoting research, development and innovation. The exchange of knowledge and constant work among various actors in society (private sector, public sector, academia, civil society) and across the different disciplines is crucial to better deal with the challenges and opportunities that this new reality brings with it.

BIBLIOGRAFÍA

ANTONOPOULOS, ANDREAS M., *Mastering Bitcoin,* 2nd Edition, O'Reilly Media. California, 2017.

ANTONOPOULOS, ANDREAS M., *Internet del Dinero,* Volume 1, Merkle Bloom LLC, MiddleTown, 2017.

ARAMENDÍA, MERCEDES, "La revolución digital: telecomunicaciones, servicios digitales y la sociedad de la información" en *Estudios de Telecomunicaciones y Sociedad de la Información,* Universidad de Montevideo, 2018.

ARAMENDÍA, MERCEDES, "Aspectos fundamentales de los servicios de telecomunicaciones en el país" en *Estudios de Telecomunicaciones y Sociedad de la Información,* Universidad de Montevideo, 2018.

ARAMEDIA, MERCEDES, "La digitalización: retos y oportunidades" en *Estudios Sobre los Desafíos Jurídicos ante la Digitalización*, Universidad de Montevideo, 2019.

ARAMENDÍA, MERCEDES, "La privacidad y las TIC", en *Estudios de Información Pública y Datos Personales,* Tomo III, Universidad de Montevideo, 2018.

BANCO MUNDIAL, "Información y Comunicación para el Desarrollo 2009: Ampliar el alcance y aumentar el impacto", 2009.

BELLO, PABLO Y SASTRE, ANDRÉS, "Re-pensar las políticas públicas para el cierre de la brecha digital en América Latina" en *Gobernanza y regulaciones de Internet en América Latina. Análisis en honor a los diez años de la South School on Internet Governance*, FGV Direito Rio, Río de Janeiro, 2018.

BRITO, MARIANO Y DELPIAZZO, CARLOS, *Derecho Administrativo de la Regulación Económica,* Universidad de Montevideo, 1998.

BRCOVITZ, RODRIGO, *Manual de propiedad intelectual*, Tirant lo Blanch, Valencia, 2012.

CAJARVILLE, JUAN PABLO, *Sobre Derecho Administrativo,* tomos I y II, Fundación de Cultura Universitaria, Montevideo, 2008.

CASTRESANA, AMELIA, *Derecho Romano. El arte de lo bueno y de lo justo.* Tercera edición, Tecnos, Madrid, 2017.

CAVANILLAS MÚGICA SANTIAGO, *Deberes y responsabilidades de los servidores de acceso y alojamiento. Un análisis multidisciplinar*, Editorial Comares, Granada, 2005.

CERISOLA, ANDRÉS, *Las telecomunicaciones en un mundo de competencia*, Eudeba, Universidad de Buenos Aires y Universidad ort, 2000.

CHECA, SUSANA, en Nota Técnica 3, "Los Derechos de Autor", Máster de Acceso a la Abogacía, Derecho Informático y Nuevas Tecnologías, Universidad de Nebrija, Año 2019.

CUADERNOS DE DERECHO JUDICIAL, ESCUELA JUDICIAL, CONSEJO GENERAL DEL PODER JUDICIAL, ¨Problemática jurídica en torno al fenómeno de internet¨, Madrid, 2000.

DAVARO, MIGUEL, *Manual de Derecho Telemático*, Thomson Aranzasi, 10º Edición, 2015.

DE MIGUEL, PEDRO ALBERTO, *Derecho privado en Internet*, Civitas, Thomson Company, Madrid, 2002.

DELPIAZZO, CARLOS, L*ecciones de Derecho Telemático*, Tomos I y II, Fundación de Cultura Universitaria.

DELPIAZZO, CARLOS, *Derecho Administrativo Especial*, vol. 2. A.M.F. Montevideo, 2009.

DELPIAZZO CARLOS Y VIEGA, MARÍA JOSÉ., *Lecciones de Derecho Telemático*, Tomo I, Fundación de Cultura Universitaria. Montevideo, 2009.

DELPIAZZO, CARLOS, *Derecho de las telecomunicaciones*, Universidad de Montevideo. Montevideo, 2005.

DELPIAZZO, CARLOS, "Regulación de Internet", en *Anuario de Derecho Informático*, Fundación de Cultura Universtaria, tomo I. 2001.

DELPIAZZO, CARLOS, "El Derecho ante las telecomunicaciones, la informática e Internet", en *Anuario de Derecho Informático*, tomo III, Fundación de Cultura Universitaria. Montevideo. 2003.

DELPIAZZO, CARLOS, "¿Hacia dónde va Internet?", en *Anuario de Derecho Informático*, tomo IV, Fundación de Cultura Universitaria. Montevideo. 2004.

DELPIAZZO, CARLOS, "Derecho y nuevas tecnologías de la información en los umbrales del siglo XXI" en *Anuario de Derecho Informático*, tomo V, Fundación de Cultura Universitaria. Montevideo. 2005.

DELPIAZZO, CARLOS, "Las nuevas tecnologías en el Uruguay. Impacto de Internet sobre la persona", en *XVº aniversario del Anuario de Derecho Administrativo*, Fundación de Cultura Universitaria. Montevideo. 2005.

DELPIAZZO, CARLOS, "Derecho de la Informática y las Telecomunicaciones", separata del XXIX Curso de Derecho Internacional (O.E.A., Washington, 2003).

DE LA FUENTE, JUAN ÁNGEL, "La tokenización de los inmuebles y el notariado", en *Revista Internacional del Notariado. Oficina Notarial Permanente de intercambio Internacional*, Buenos Aires, 2018.

DURÁN, AUGUSTO, "Competencia de ANTEL", en *Estudios de Derecho Público*, volumen I, Mastergraf. Montevideo. 2004.

DURÁN MARTÍNEZ, AUGUSTO, *Contencioso Administrativo*, Fundación de Cultura Universitaria. Montevideo. 2007.

ECHEBERRÍA, RAÚL, "Construyendo modelos innovadores de gobernanza" en *Gobernanza y regulaciones de Internet en América Latina. Análisis en honor a los diez años de la South School of Internet Governance*, FGV Direito Rio. Río de Janeiro, 2018.

ETLA: Smart Contracts - How will Blockchain Technology Affect Contractual Practices - The Research Institute if the Finnish Economy Nº 68, 2017.

GAMARRA, JORGE, *Tratado de Derecho Civil Uruguayo Tomo XI -Doctrina General del Contrato*, Vol. 4, Segunda edición, Fundación de Cultura Universitaria, Montevideo, 1999.

GAMARRA, JORGE, *Tratado de Derecho Civil Uruguayo, Tomo XVII, Responsabilidad Contractual*, Vol. 1, segunda edición, Fundación de Cultura Universitaria, Montevideo, 1992.

GAUTHIER, Gustavo, *Disrupción, economía compartida y derecho: enfoque jurídico multidisciplinario*, Fundación de Cultura Uruguaya, Montevideo, 2016.

GOODMAN, MARC, *Future Crimes. Inside the digital underground and the Battle for Our Connected World*, Anchor Books, United States, New York, 2016.

GRIMMELMANN, JAMES, *Internet Law*, Semaphore Press, 2019.

KATZ, RAÚL, *El ecosistema y la economía digital en América Latina*, Ariel y Fundación Telefónica, Madrid, 2015.

KARLYN, MATT, profesor invitado en Cornell Tech, quien dictó el 13 de noviembre de 2019 una clase denominada "*Integrating Information security into de the contracting process*".

LLOYD, IAN, *Information Technology Law*, Oxford, 8th Edition, 2017.

MARTINEZ, NURIA, *Los fines educativos y de investigación como límite al derecho de autor*, DYKINSON, Madrid, 2018, p. 64.

MAYER-SCHÖNBERGER, VIKTOR Y CUKIER, KENNETH, *Big Data - A Revolution that will transform how we live, work and think*, Gran Bretaña, 2013.

MURRAY, ANDREW, *Information Technology Law. The Law and Society*, Oxford University Press. 2013.

MURRAY, ANDREW, *Information Technology Law. The Law and Society*, Third edition, Oxford University Press, Oxford, 2018.

Navas, Susana, *Inteligencia artificial. Tecnología. Derecho*, Tirant lo Blanch. Valencia, 2017.

Navas, SUSANA, *Mercado Digital Principios y Reglas Jurídicas*, Tirant lo Blanch, Valencia, 2016.

Navas, SUSANA, *La Personalidad Virtual del Usuario de Internet*, Tirant lo Blanch, Valencia, 2014.

NOAH HARARI, YUVAL, *Homo Deus - Breve Historia del mañana*. Debate. Barcelona, 2016.

PAZA PENDÉS JAVIER y MARTÍNEZ VELENCOSO LUZ, *Nuevos retos jurídicos de la Sociedad Digital*, Thomson Reuters, Aranzadi, Navarra, 2017.

PÉREZ BES, FRANCISCO, *El Derecho de Internet* - (Coordinador) - Atelier Libros Jurídicos. Barcelona, 2016.

PEREZ-SERRABONA GONZALEZ, JOSE LUIS, *Entorno a la interpretación de las condiciones generales del seguro*, Editorial Universidad de Granada, España, 1987.

PEREZ-SERRABONA GONZALEZ, JOSE LUIS: *Derecho de Sociedades y otros operadores del mercado*, Editorial Téncica Avicam, España, 2015.

PORRAS, BERNARDO, *La telefonía es actividad de libre competencia,* en *Revista Tribuna del Abogado,* Nº 132. Montevideo. 2003.

PUYOL, JAVIER, *Aproximación jurídica y económica al big data*, Tirant lo Blanch, Valencia, 2015.

RAMOS, JOAN, *Propiedad Digital, la cultura en Internet como objeto de cambio*, Editorial Trotta, 2018.

ROSELLÓ, FRANCISCA, *Cloud Computing. Régimen Jurídico para Empresarios*. Thomson Reuters. Aranzadi. 2018.

SANJURJO, BEATRIZ, *Manual de Internet y Redes Sociales*, Dykinson, 2015.

SAROT, PABLO, "La Economía Digital", en *Revista de Negocios del ieem,* N° 2, Montevideo, 2016.

SCHIAVI, PABLO, *Estudios de Información Pública y Datos Personales* (Tomo III), Universidad de Montevideo, 2019.

SCHIAVI PABLO, "Protección de los datos personales en las redes sociales", en Estudios de Derecho Administrativo, nº 7, 2013.

SIGÜENZA, ALICIA, "La libertad de expresión en Internet" en *El Derecho de Internet.* Atelier Libros Jurídicos, Valencia, 2016.

STECK, CHRISTOPH, *Manifiesto Digital. Por una Internet abierta y segura para todos*, Telefónica S.A., 2015.

TAPSCOTT, DON Y TAPSCOTT, ALEX, *La Revolución Blockchain,* Deusto, Barcelona, 2017.

TUR FAÚNDEZ, CARLOS, *Derecho de las nuevas tecnologías. Smart Contracts Análisis Jurídico,* Ed. Reus, Madrid, 2018.

VALLS PRIETO, JAVIER, *Retos Jurídicos por la Sociedad Digita¨*, Thomson Reuters, Aranzadi, 2018.

VARGAS, FERNANDO, “La nueva economía digital”, en *Tribuna del abogados*, Nº 197, Montevideo, 2016.

Vázquez, CRISTINA, “Procedimientos Administrativos. Decreto 500/991 de 27 de setiembre de 1991”, en *La Ley Uruguay*, Montevideo, 2013

BIBLIOGRAFÍA ONLINE:

AGENDA DIGITAL PARA EUROPA. url: https://www.europarl.europa.eu/factsheets/es/sheet/64/digital-agenda-for-europe Consultado el 15 de enero de 2019.

AGENDA DIGITAL PARA AMÉRICA LATINA Y EL CARIBE (elac2020). url: https://conferenciaelac.cepal.org/6/sites/elac2020/files/cmsi.6_agenda_digital.pdf Consultado el 15 de enero de 2019.

AGENDA DIGITAL URUGUAY 2020. url: https://www.impo.com.uy/diariooficial/2017/01/23/3 Consultado el 15 de enero de 2019.

AGENDA ESPAÑOLA DE PROTECCIÓN DE DATOS. URL: https://www.agpd.es/portalwebAGPD/temas/reglamento/common/pdf/directricesportabilidad.pdf . Consultado 20 de octubre de 2018.

AGENCIA DE GOBIERNO ELECTRÓNICO Y SOCIEDAD DE LA INFORMACIÓN Y DEL CONOCIMIENTO. (AGESIC). URL: https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/comunicacion/noticias/uruguay-nueva-zelanda-israel-crean-prototipo-para-traducir-leyes-codigo Consultado el 25 de febrero de 2019.

AGENCIA DE GOBIERNO ELECTRÓNICO Y SOCIEDAD DE LA INFORMACIÓN Y DEL CONOCIMIENTO (AGESIC), Marco de Ciberseguridad 4.0, URL: https://archivos.agesic.gub.uy/nextcloud/index.php/s/cgbssgiLEopFcRm#pdfviewer Consultado el 20 de enero de 2020.

AGENCIA DE GOBIERNO ELECTRÓNICO Y SOCIEDAD DE LA INFORMACIÓN Y DEL CONOCIMIENTO. (AGESIC), https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/tramites-y-servicios/servicios/centro-de-operaciones-de-seguridad-soc Consultado el 31 de enero de 2020.

AGENCIA DE GOBIERNO ELECTRÓNICO Y SOCIEDAD DE LA INFORMACIÓN Y DEL CONOCIMIENTO (AGESIC), https://www.gub.uy/centro-nacional-respuesta-incidentes-seguridad-informatica/institucional/cometidos/division-centro-de-operaciones-de-ciberseguridad-soc Consultado el 31 de enero de 2020.

AGENCIA DE GOBIERNO ELECTRÓNICO Y SOCIEDAD DE LA INFORMACIÓN Y DEL CONOCIMIENTO (AGESIC), Seguridad en IoT, Proceso en Uruguay, Setiembre 2019. URL: https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/comunicacion/publicaciones/seguridad-iot Consultado el 20 de enero de 2020.

BAKERLAW,https://www.bakerlaw.com/webfiles/Privacy/2018/Articles/CCPA-GDPR-Chart.pdf Consultado el 13 de mayo de 2020.

BBVA: Todo lo que hay que saber de la psd2. URL: https://www.bbva.com/es/lo-saber-la-psd2/ Consultado el 25 de febrero de 2019.

BBVA: URL: https://www.bbva.com/es/que-es-un-sandbox-regulatorio/ Consultado: 15 noviembre 2018.

BLOOMBERG, https://www.bloomberg.com/news/features/2019-08-07/section-230-was-supposed-to-make-the-internet-a-better-place-it-failed Consultado el 13 de mayo de 2020.

BID Y FINNOVISTA: fintech: Innovaciones que no sabías que eran de América Latina y Caribe, 2017. URL: https://publications.iadb.org/es/fintech-innovaciones-que-no-sabias-que-eran-de-america-latina-y-caribe Consultado: 15 noviembre 2019.

BID Y FINNOVISTA: fintech: Innovaciones que no sabías que eran de América Latina y Caribe, 2018. URL: https://publications.iadb.org/es/fintech-america-latina-2018-crecimiento-y-consolidacion Consultado: 15 noviembre 2019.

BID: ¨Servicios sociales para ciudadanos digitales. Oportunidades para América Latina y el Caribe¨. URL: https://publications.iadb.org/es/servicios-sociales-para-

ciudadanos-digitales-oportunidades-para-america-latina-y-el-caribe Consultado el 20 de febrero de 2019.

BURR & FORMN LLP: Uniform Regulation of Virtual-Currency Businesses Act Offers States Regulatory Framework for the Virtual Currency Industry. URL: https://www.burr.com/blogs/blockchain-law/2018/05/18/uniform-regulation-of-virtual-currency-businesses-act-offers-states-regulatory-framework-for-the-virtual-currency-industry/ 53ce4ec21410 Consultado el 25 de febrero de 2019.

BUGALLO, BEATRIZ, "Manual de Propiedad Intelectual". URL: https://drive.google.com/file/d/1rE92X76p2GHXEHoEFcF_6mmQTpO3OY1e/view Consultado el 20 de enero de 2020.

CABELLO, SEBASTIÁN, UNIVERSIDAD DE SAN ANDRÉS: "Documento de trabajo N. 2019-4. Centro de Estudios en Tecnología y Sociedad". "La nueva regulación europea de Copyright: ejes clave para el debate en América Latina". URL: http://repositorio.udesa.edu.ar/jspui/bitstream/10908/16695/1/%5BP%5D%5BW%5D%20-%20Cabello%2C%20Sebasti%C3%A1n%20M..pdf _ Consultado el 20 de enero de 2020.

CEPAL: Lecuona, Ramón "Inclusión financiera de las PYMEs en México" https://www.cepal.org/sites/default/files/events/files/inclusion_financiera_de_las_pymes_en_mexico._ramon_lecuona.pdf Consultado: 11 de Noviembre 2018.

Ciberseguridad, URL: https://www.dsn.gob.es/es/sistema-seguridad-nacional/qu%C3%A9-es-seguridad-nacional/%C3%A1mbitos-seguridad-nacional/ciberseguridad Consultado el 31 de enero de 2020.

CNMC: Comisión Nacional de los Mercados y la Competencia. URL: https://www.cnmc.es/sites/default/files/1533234_0.pdf Consultado el 5 de octubre de 2017.

CNMC: COMISIÓN NACIONAL DE LA COMPETENCIA Y LOS MERCADOS, España (2018) Estudio sobre el impacto en la competencia de las nuevas tecnologías en el sector financiero (Fintech). Disponible en: https://www.cnmc.es/sites/default/files/2173343_12.pdf Consultado el 15 de enero de 2019.

Código Europeo de Comunicaciones Electrónicas. url: https://eur-lex.europa.eu/legal-content/ES/ALL/?uri=CELEX:52016PC0590 Consultado el 9 de febrero de 3029.

COMISIÓN EUROPEA, Las nuevas normas sobre servicios de pago beneficiarán a los consumidores y a los minoristas. URL: http:// https://ec.europa.eu/commission/presscorner/detail/es/IP_13_730 Consultado el 25 de febrero de 2019.

COMISIÓN EUROPEA, Comunicado de prensa. url: http://europa.eu/rapid/press-release_IP-15-4919_es.htm Consultado el 15 de enero de 2019.

COMISIÓN EUROPEA, Comunicado de Prensa. url: http://europa.eu/rapid/press-release_IP-17-1232_es.htm Consultado el 15 de enero de 2019.

COMISIÓN EUROPEA, Plataformas en línea. url: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A52016DC0288 Consultado el 15 de enero de 2019.

COMISIÓN EUROPEA, el Mercado Único Digital. url: http://publications.europa.eu/webpub/com/factsheets/digital/es/#what-is-digital-single-market Consultado el 15 de enero de 2019.

COMISIÓN EUROPEA, Comunicado de prensa. url: http://europa.eu/rapid/press-release_IP-18-3742_es.htm Consultado el 15 de enero de 2019.

COMISIÓN EUROPEA, Consulta Pública relativa a la reutilización de la información del sector público. url: https://ec.europa.eu/info/consultations/public-consultation-review-directive-re-use-public-sector-information-psi-directive_es Consultado el 15 de enero de 2019.

COMISIÓN EUROPEA, Comunicación de la Comisión Europea, com/2016/0288 final, URL: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A52016DC0288 Consultado el 20 de febrero de 2019.

COMISIÓN EUROPEA, Comunicado de Prensa: “Plataformas en línea: la Comisión establece nuevas normas sobre transparencia y equidad”. url: https://ec.europa.eu/digital-single-market/en/news/regulation-promoting-fairness-and-transparency-business-users-online-intermediation-services Consultado el 20 de febrero de 2019.

COMISIÓN INTERAMERICANA DE DERECHOS HUMANOS en *"Estándares para una Internet Libre, Abierta e Incluyente".* URL: http://www.oas.org/es/cidh/expresion/docs/publicaciones/INTERNET_2016_ESP.pdf Consultado el 20 de febrero de 2019.

CONSEJO DE EUROPA: ¨Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data¨, URL: https://rm.coe.int/16806ebe7a Consultado el 20 de febrero de 2019.

CONSEJO DE LA UNIÓN EUROPEA, URL: https://www.consilium.europa.eu/es/press/press-releases/2019/05/17/cyber-attacks-council-is-now-able-to-impose-sanctions/Consultado el 31 de enero de 2020.

CORTE INTERAMERICANA DE DERECHOS HUMANOS, Informe No 112/2012, Caso 12.828. URL: https://www.corteidh.or.cr/docs/casos/granier_otros/esap.pdf Consultado el 20 de febrero de 2019.

COUNCIL OF THE EUROPEAN UNION, Council Conclusions on the significance of 5G to the European Economy and the need to mitigate security risks linked to 5G. URL: https://www.consilium.europa.eu/media/41595/st14517-en19.pdf Consultado el 31 de enero de 2020.

COURSERA: Digital Transformation. Dictado por Boston Consulting Group junto con University of Virginia, Darden School of Business. url: https://www.coursera.org/learn/bcg-uva-darden-digital-transformation/lecture/a7T8h/exponential-evolution-of-technology Consultado el 4 de enero de 2019.

COMISIÓN EUROPEA, Comunicado de prensa. url: http://europa.eu/rapid/press-release_IP-15-4919_es.htm Consultado el 15 de enero de 2019.

COMISIÓN EUROPEA, Comunicado de Prensa. url: http://europa.eu/rapid/press-release_IP-17-1232_es.htm Consultado el 15 de enero de 2019.

COMISIÓN EUROPEA, el Mercado Único Digital. url: http://publications.europa.eu/webpub/com/factsheets/digital/es/#what-is-digital-single-market Consultado el 15 de enero de 2019.

COMISIÓN EUROPEA, Comunicado de prensa. url: http://europa.eu/rapid/press-release_IP-18-3742_es.htm Consultado el 15 de enero de 2019.

COMISIÓN EUROPEA, Consulta Pública relativa a la reutilización de la información del sector público. url: https://ec.europa.eu/info/consultations/public-consultation-review-directive-re-use-public-sector-information-psi-directive_es Consultado el 15 de enero de 2019.

CONVENIO SOBRE LA CIBERDELINCUENCIA, BUDAPEST, 22 de noviembre de 2001. URL: https://www.oas.org/juridico/english/cyb_pry_convenio.pdf Consultado el 20 de enero de 2020.

CUMBRE MUNDIAL SOBRE LA SOCIEDAD DE LA INFORMACIÓN, url: https://www.itu.int/net/wsis/geneva/index-es.html Consultado el 10 de febrero de 2019.

CUMBRE MUNDIAL SOBRE LA SOCIEDAD DE LA INFORMACIÓN, url: https://www.itu.int/net/wsis/tunis/index-es.html Consultado el 9 de febrero de 2019.

DATAGUIDANCE, https://fpf.org/wp-content/uploads/2018/11/GDPR_CCPA_Comparison-Guide.pdf Consultado el 13 de mayo de 2020.

DECLARACIÓN UNIVERSAL DE DERECHOS HUMANOS, URL: https://www.un.org/es/universal-declaration-human-rights/ Consultado el 20 de febrero de 2019.

DICCIONARIO DE LA REAL ACADEMIA ESPAÑOLA:

Definición de "Contexto", 2., url: http://dle.rae.es/?id=AVBbFZW Consultado el 15 de enero de 2019.

Definición de "Revolución", url: http://dle.rae.es/?id=WQ0Bykx Consultado el 4 de octubre de 2017.

Definición de "Digital", url: http://dle.rae.es/?id=Dl56Lag Consultado el 4 de octubre de 2017.

Definición de "Digitalización". url: http://dle.rae.es/?id=Dl5l0Y6 Consultado el 15 de enero de 2019.

Definición de "Digitalizar". url: http://dle.rae.es/?id=DlBB81T Consultado el 15 de enero de 2019.

Definición de “Bit”, Diccionario de la Real Academia Española. url: http://dle.rae.es/?id=5cPrUzM Consultado el 15 de enero de 2019.

Definición de Red: url: https://dle.rae.es/?w=red consultado el 7 de febrero de 2019.

Definición de Tele. http://dle.rae.es/?id=ZLKsvGW|ZLLzOPm Consultado el 28 de octubre de 2017.

Definición de Internet. url: https://dle.rae.es/?id=LvskgUG Consultado el 7 de febrero de 2019.

Definición de “Derechos fundamentales”: http://dle.rae.es/?id=CGv2o6x Consultado el 7 de febrero de 2019.

Definición de “Propiedad Intelectual”: URL: https://dle.rae.es/propiedad Consultado el 18 de diciembre de 2019.

DICCIONARIO DE OXFORD, de noción de “cryptocurrency”. URL: https://www.oxfordlearnersdictionaries.com/definition/english/cryptocurrency Consultado el 20 de febrero de 2019.

BANCO CENTRAL EUROPEO, Dictamen de 12 de octubre de 2016, sobre una propuesta de directiva del Parlamento Europeo y del Consejo por la que se modifica la Directiva (UE) 2015/849 relativa a la prevención de la utilización del sistema financiero para el blanqueo de capitales o la financiación del terrorismo, y por la que se modifica la Directiva 2009/101/CE (CON/2016/49). URL: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A52016AB0049 Consultado el 20 de febrero de 2019.

CAMBRIDGE DICTIONARY, URL: https://dictionary.cambridge.org/dictionary/english/hate-speech Consultado el 13 de mayo de 2020.

Directiva (UE) 2018/843 del Parlamento Europeo y del Consejo de 30 de mayo de 2018. URL: https://eur-lex.europa.eu/legal-content/es/TXT/?uri=CELEX%3A32018L0843 Consultado el 15 de enero de 2020.

Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo de 6 de julio de 2016 relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión. url:

https://www.boe.es/doue/2016/194/L00001-00030.pdf . Consultado el 15 de enero de 2019.

Directiva (ue) 2018/1972 del Parlamento Europeo y del Consejo, de 11 de diciembre de 2018, por la que se establece el Código de las Comunicaciones Electrónicas. url: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:32018L1972 Consultado el 15 de enero de 2019.

Directiva (UE) 2019/789 del Parlamento Europeo y del Consejo de 17 de abril de 2019 por la que se establecen normas sobre el ejercicio de los derechos de autor y derechos afines aplicables a determinadas transmisiones en línea de los organismos de radiodifusión y a las retransmisiones de programas de radio y televisión. URL: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:32019L0789 Consultado el 20 enero de 2020.

El Pais, URL: https://negocios.elpais.com.uy/noticias/banco-central-tomo-resolucion-denuncia-paganza-itau.html Consultado el 20 de febrero de 2019.

EL PAIS, por qué grandes organizaciones recomiendan no usar Whatsapp. URL: https://elpais.com/tecnologia/2020/01/31/actualidad/1580429952_417173.html Consultado el 31 de enero de 2020.

ENISA, Good practices in the implementation of regulatory technical standards. url: https://www.enisa.europa.eu/news/enisa-news/good-practices-in-the-implementation-of-regulatory-technical-standards Consultado el 15 de enero de 2019.

FACEBOOK, INC: https://about.fb.com/wp-content/uploads/2020/03/March-18-2020-Press-Call-Transcript.pdf Consultado el 13 de mayo de 2020.

FERNANDEZ CESPEDES, PATRICIA. “El hombre contra la máquina, ¿puede un robot ostentar derechos de propiedad intelectual?. URL: https://www.bamboo.legal/inteligencia-artificial-derechos-de-autor/ Consultado el 20 de enero de 2020.

FUNDÉU BBVA, recomendaciones tras búsqueda “digital”. url: https://www.fundeu.es/recomendacion/online-conectado-digital-electronico-o-en-linea-1416/ Consultado el 15 de enero de 2019.

GOBIERNO DE ESPAÑA, Estrategia Nacional de Ciberseguridad, Gobierno de España, julio 2019, URL: https://www.dsn.gob.es/es/documento/estrategia-nacional-ciberseguridad-2019 Consultado el 31 de enero de 2020.

GRANT THORNTON: RGPD y Blockchain. Soluciones blockchain para el Reglamento General de Protección de datos. URL: https://www.grantthornton.es/globalassets/___spain___/folletos/rgpd-y-blockchain-final.pdf Consultado el 20 de octubre de 2018.

IAPP EUROPE DATA PROTECTION CONGRES ONLINE: https://iapp.org/ Consultado el 20 de octubre de 2019.

INFOCYTE. Cybersecurity 101: Introducción a los 10 tipos más comunes de ataques de ciberseguridad. URL: https://www.infocyte.com/es/blog/2019/05/01/cybersecurity-101-intro-to-the-top-10-common-types-of-cyber-security-attacks/ Consultado el 25 de enero de 2020.

MEJIA LLANO, Juan Carlos en¨Estadísticas de redes sociales 2018...¨. URL: https://www.juancmejia.com/marketing-digital/estadisticas-de-redes-sociales-usuarios-de-facebook-instagram-linkedin-twitter-whatsapp-y-otros-infografia/ Consultado el 20 de octubre de 2018.

Ministerio De Educación Y Cultura De Uruguay, Mensaje del Proyecto de ley sobre el Derecho de Autor y Derechos afines, Ministerio de Educación y Cultura de Uruguay. Mayo 2000. URL: http://archivo.presidencia.gub.uy/noticias/archivo/2000/mayo/2000052300.htm Consultado el 20 de enero de 2020.

JUAN, NICOLÁS Y ARIAS, CECILIA: "Uruguay lidera tributación para plataformas digitales". URL: https://www.uruguayxxi.gub.uy/es/noticias/articulo/uruguay-lidera-tributacion-para-plataformas-digitales/ Consultado el 20 de febrero de 2019.

KMPG - "The Pulse of Fintech 2018 - Biannual global analysis of investment in Fintech" URL - https://assets.kpmg.com/content/dam/kpmg/xx/pdf/2018/07/h1-2018-pulse-of-Fintech.pdf Consultado: 11 de noviembre 2018

KMPG - “Fintech, innovación al servicio del cliente” URL - https://assets.kpmg.com/content/dam/kpmg/es/pdf/2017/11/Fintech-innovacion-servicio-cliente.pdf Consultado: 11 de noviembre 2018.

La Diaria, URL: https://ladiaria.com.uy/articulo/2018/8/banco-central-debera-laudar-por-conflicto-entre-itau-y-paganza Consultado el 20 de febrero de 2019.

LACALLA POU, Anteproyecto de Ley de Urgente Consideración, URL: https://lacallepou.uy/anteproyectoLUC.pdf Consultado el 20 de enero de 2020.

LIBRO BLANCO FINTECH, URL - https://solucionesconfirma.es/observatorio/wp-content/uploads/LibroBlancoFintech.pdf Consultado: 11 de noviembre 2018.

Quora, “Everything you need to know about the top five fintech trends of 2018”. url: https://www.forbes.com/sites/quora/2018/09/25/everything-you-need-to-know-about-the-top-five-FINTECH-trends-of-2018/#35798c666b93 Consultado el 20 de febrero de 2019.

HOMELAND SECURITY, Sectores de infraestructura crítica: https://www.dhs.gov/cisa/critical-infrastructure-sectors referenciado en OEA-AWS-Marco NIST de ciberseguridad, URL: https://www.oas.org/es/sms/cicte/docs/OEA-AWS-Marco-NIST-de-Ciberseguridad-ESP.pdf Consultado el 20 de enero de 2020.

INTERNET SOCIETY, url: https://www.Internetsociety.org/es/Internet/ Consultado el 7 de febrero de 2019.

INTERNET SOCIETY, url: https://www.Internetsociety.org/es/about-the-Internet/how-it-works/ Consultado el 7 de febrero de 2019.

INTERNET SOCIETY, URL: https://www.Internetsociety.org/es/Internet/history-Internet/brief-history-Internet/ Consultado el 8 de febrero de 2019.

INTERNET SOCIETY, “Breve Historia de Internet” realizado por Barry M. Leiner, Vinton G. Cerf, David D. Clark, Robert. E. Kahn, Leonard Kleinrock, Daniel C. Lynch, Jon Postel, Larry G. Roberts, Stephen Wolff. url: https://www.Internetsociety.org/es/Internet/history-Internet/brief-history-Internet Consultado el 9 de febrero de 2019.

NACIONES UNIDAS, Objetivos de Desarrollo Sostenible. url: http://www.undp.org/content/undp/es/home/sustainable-development-goals.html Consultado el 15 de enero de 2019.

NACIONES UNIDAS, El derecho a la privacidad en la era digital, Res.69/166. URL: https://ap.ohchr.org/documents/S/HRC/d_res_dec/A_HRC_28_L27.pdf Consultado el 20 de febrero de 2019.

NACIONES UNIDAS Y OTROS, ¨Declaración Conjunta sobre libertad de expresión e Internet¨. URL: http://www.oas.org/es/cidh/expresion/showarticle.asp?artID=849&lID=2 Consultado el 11 de marzo de 2019.

NACIONES UNIDAS, Asamblea General. Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión, Frank La Rue. A/HRC/17/27. 16 de mayo de 2011. URL: https://www.acnur.org/fileadmin/Documentos/BDL/2015/10048.pdf?view=1 Consultado el 20 de febrero de 2019.

NEW YORK TIMES, CHRIS STOKEL-WALKER: "Algorithms Won't Fix What's Wrong With Youtube" https://www.nytimes.com/2019/06/14/opinion/youtube-algorithm.html?auth=login-email&login=email Consultado el 13 de mayo de 2020.

NEW YORK TIMES, https://www.nytimes.com/2019/08/06/technology/section-230-hate-speech.html Consultado el 13 de mayo de 2020.

Nota de prensa: NYTIMES: https://www.nytimes.com/2012/02/19/magazine/shopping-habits.html Consultado el 20 de febrero de 2019.

NOAH HARARI, YUVAL, *"Homo Deus - Breve Historia del mañana"*. URL: https://www.beek.io/frases/homo-deus-breve-historia-del-manana Consultado el 10 de diciembre de 2020.

OEA Y AWS, Ciberseguridad, Marco NIST. URL: https://www.oas.org/es/sms/cicte/docs/OEA-AWS-Marco-NIST-de-Ciberseguridad-ESP.pdf Consultado el 20 de enero de 2020.

OECD, URL: https://www.oecd.org/ctp/beps-resumen-informativo.pdf Consultado el 20 de febrero de 2019.

OECD: The Digital Economy. URL:http://www.oecd.org/daf/competition/The-Digital-Economy-2012.pdf Año 2012. Consultado el 20 de febrero de 2019.

OECD: "Big Data: Bringing Competition Policy to the Digital Era". URL: https://one.oecd.org/document/DAF/COMP(2016)14/en/pdf Año 2016. Consultado el 20 de febrero de 2019.

OECD: Perspectivas de la OCDE sobre la economía digital 2017. Disponible en: https://read.oecd-ilibrary.org/science-and-technology/perspectivas-de-la-ocde-sobre-la-economia-digital-2017_9789264302211-es#page8 Año 2017. Consultado el 20 de febrero de 2019.

OECD: Rethinking the Use of Traditional Antitrust Enforcement Tools in Multi-Sided markets. Disponible en: https://www.oecd.org/daf/competition/Rethinking-antitrust-tools-for-multi-sided-platforms-2018.pdf Año 2017. Consultado el 20 de febrero de 2019.

OECD: Algorithms and Collusion - Background note from the Secretariat. Disponible en: http://www.oecd.org/daf/competition/Algorithms-and-colllusion-competition-policy-in-the-digital-age.pdf Año 2017. Consultado el 20 de febrero de 2019.

OECD Directrices para la seguridad de sistemas y redes de información: Hacia una cultura de seguridad. URL: https://www.oecd.org/sti/ieconomy/34912912.pdf Consultado el 20 de enero de 2020.

OECD: Recomendación del Consejo en su 1037 sesión del 25 de julio de 2002. URL: https://www.oecd.org/sti/ieconomy/34912912.pdf Consultado el 31 de enero de 2020.

OECD. Working Party on Information Security and Privacy. Implementation Plan for the OECD guidelines for the security of information system and networks: towards a culture of security. URL: http://www.oecd.org/internet/ieconomy/31670189.pdf Consultado el 20 de enero de 2020.

OECD Digital Economy Papers No. 102: The Promotion of a Culture of Security for Information Systems and Networks in OECD Countries. URL: https://www.oecd-ilibrary.org/docserver/232017148827.pdf?expires=1579684789&id=id&accname=guest

&checksum=5DA1786E44A7AE2307B088EF3858CC8B Consultado el 20 de enero de 2020.

OMPI: https://www.wipo.int/about-ip/es/ Consultado el 14 de enero de 2020.

OMPI: ¿Qué es la Propiedad Intelectual?. URL: https://www.wipo.int/about-ip/es/ Consultado el 14 de enero de 2020.

PARLAMENTO EUROPEO, URL: http://www.europarl.europa.eu/factsheets/es/sheet/43/el-mercado-unico-digital-omnipresente Consultado el 15 de enero de 2019.

PARLAMENTO EUROPEO, Normas de Derecho Civil sobre robótica. URL: https://www.europarl.europa.eu/doceo/document/TA-8-2017-0051_ES.pdf?redirect Consultado el 20 de enero de 2020.

PARLAMENTO EUROPEO, sobre una política industrial global europea en materia de inteligencia artificial y robótica (2018/2088(INI)). URL: https://www.europarl.europa.eu/doceo/document/A-8-2019-0019_ES.html Consultado el 20 de enero de 2020.

PARLAMENTO DE LA REPÚBLICA ORIENTAL DEL URUGUAY, Proyecto de Ley presentado por Tabaré Viera. URL: https://parlamento.gub.uy/documentosyleyes/ficha-asunto/103462/ficha_completa Consultado el 20 de enero de 2020.

PRESIDENCIA DE LA REPÚBLICA ORIENTAL DEL URUGUAY, https://medios.presidencia.gub.uy/legal/2018/decretos/05/mef_1835.pdf ◇ Consultado el 20 de febrero de 2019.

PRESIDENCIA DE LA REPÚBLICA ORIENTAL DEL URUGUAY, URL: https://www.presidencia.gub.uy/comunicacion/comunicacionnoticias/seguridad-informatica-proyecto-ley Consultado el 20 de enero de 2020.

PRINCIPIOS DE MANILA SOBRE RESPONSABILIDAD DE LOS INTERMEDIARIOS. URL: https://www.eff.org/files/2015/06/23/manila_principles_1.0_es.pdf Consultado el 20 de febrero de 2019.

PROGRAMA DE ACTIVIDADES DE COOPERACIÓN REGIONAL DE LA AGENDA DIGITAL PARA AMÉRICA LATINA Y EL CARIBE, 2018-2020. url:

https://www.cepal.org/sites/default/files/static/files/programa_de_actividades_elac2020_0.pdf Consultado el 15 de enero de 2019.

PROPUESTA DE REGLAMENTO SOBRE EL RESPETO DE LA VIDA PRIVADA Y LA PROTECCIÓN DE LOS DATOS PERSONALES EN EL SECTOR DE LAS COMUNICACIONES ELECTRÓNICAS. url: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A52017PC0010 Consultado el 15 de enero de 2019.

PROPUESTA DE REGLAMENTO DEL PARLAMENTO EUROPEO Y DEL CONSEJO RELATIVO A UN MARCO PARA LA LIBRE CIRCULACIÓN DE DATOS NO PERSONALES EN LA UNIÓN EUROPEA. url: https:// https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:52017PC0495 Consultado el 15 de enero de 2019.

PROPUESTA DE DIRECTIVA DEL PARLAMENTO EUROPEO Y DEL CONSEJO SOBRE LOS DERECHOS DE AUTOR EN EL MERCADO ÚNICO DIGITAL, COM/2016/0593 final – 2016/0280 (COD). URL: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A52016PC0593 Consultado el 20 de enero de 2020.

PROYECTO DE LEY REMITIDO POR EL PODER EJECUTIVO DE URUGUAY, en marzo de 2016. URL: https://parlamento.gub.uy/documentosyleyes/ficha-asunto/128667 Consultado el 20 de febrero de 2019.

PROYECTO DE LEY PRESENTADO POR CEDU Y CUTI: URL: https://www.cedu.org.uy/cedu-y-cuti-presentaron-proyecto-de-ley-para-promover-la-economia-colaborativa/ Consultado el 20 de febrero de 2019.

REGLAMENTO RELATIVO A UN MARCO PARA LA LIBRE CIRCULACIÓN DE DATOS NO PERSONALES EN LA UE. url: http://data.consilium.europa.eu/doc/document/PE-53-2018-INIT/en/pdf Consultado el 15 de enero de 2019.

REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO , de 27 de abril de 2016, 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 (Reglamento general de protección de datos).

url: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32016R0679 Consultado el 15 de enero de 2019.

STOKEL-WALKER, CHRIS, https://www.wired.co.uk/article/coronavirus-facts-moderators-facebook-youtube Consultado el 13 de mayo de 2020.

STOKEL-WALKER, CHRIS, URL: https://www.wired.co.uk/article/coronavirus-facts-moderators-facebook-youtube Consultado el 13 de mayo de 2020.

UNESCO. Fostering Freedom Online: The role of Internet Intermediaries. Unesco Series on Internet Freedom. Internet Society (2014). URL: https://unesdoc.unesco.org/ark:/48223/pf0000231162 Consultado el 20 de febrero de 2019.

UNIÓN INTERNACIONAL DE TELECOMUNICACIONES, URL: https://www.itu.int/net/ITU-R/asp/terminology-definition.asp?lang=es&rlink={03A8C3A6-D1F1-4B8C-B27C-CA20B0139DF6} Consultado el 7 de febrero de 2019.

UNIÓN INTERNACIONAL DE TELECOMUNICACIONES, URL: https://www.itu.int/net/ITU-R/asp/terminology-definition.asp?lang=es&rlink={5B1E44AD-78E4-4190-B129-376DEA4D2E44} Consultado el 7 de febrero de 2019.

UNIÓN INTERNACIONAL DE TELECOMUNICACIONES, URL: https://www.itu.int/es/about/Pages/default.aspx Consultado el 5 de febrero de 2018.

UNIÓN INTERNACIONAL DE TELECOMUNICACIONES, KATZ, RAUL: "Social and Economic Impact of Digital Transformation on the Economy". Julio 2017. url: https://www.itu.int/en/ITU-D/Conferences/GSR/Documents/GSR2017/Soc_Eco_impact_Digital_transformation_finalGSR.pdf Consultado el 30 de enero de 2019.

UNIÓN INTERNACIONAL DE TELECOMUNICACIONES, URL:https://www.itu.int/net/wsis/basic/faqs_answer.asp?lang=es&faq_id=42 Consultado el 5 de octubre de 2017.

UNIÓN INTERNACIONAL DE TELECOMUNICACIONES,, Información de referencia sobre el Plan Estratégico de la Unión para 2016-2019. URL:

https://www.itu.int/en/council/planning/Documents/Background_Strategic%20Plan%20for%20the%20Union%202016-2019_Spanish.pdf Consultado el 20 de enero de 2020.

UNIÓN INTERNACIONAL DE TELECOMUNICACIONES, Reglamento de Radiocomunicaciones de la UIT,Volumen 1, Capítulo 1: terminología y características técnicas. URL: http://search.itu.int/history/HistoryDigitalCollectionDocLibrary/1.43.48.es.301.pdf Consultado el 15 de enero de 2019.

UNIÓN INTERNACIONAL DE TELECOMUNICACIONES, Directrices de política y aspectos Económicos de Asignación y Uso del Espectro Radioeléctrico. url: https://www.itu.int/dms_pub/itu-d/opb/pref/D-PREF-EF.RAD_SPEC_GUIDE-2016-PDF-S.pdf Consultado el 20 de febrero de 2019.

UNIÓN INTERNACIONAL DE TELECOMUNICACIONES, Declaración de Principios de Ginebra de la Cumbre Mundial sobre la Sociedad de la Información. url: https://www.itu.int/net/wsis/docs/geneva/official/dop-es.html Consultado el 20 de febrero de 2019.

UNIÓN INTERNACIONAL DE TELECOMUNICACIONES, Sobre la uit: https://www.itu.int/es/about/Pages/default.aspx . Consultado el 5 de febrero de 2018.

UNIÓN INTERNACIONAL DE TELECOMUNICACIONES, Resolución Nº 9 del 2014. url: https://www.itu.int/dms_pub/itu-d/opb/stg/D-STG-SG02.RES09.1-2014-PDF-S.pdf . Consultado el 20 de febrero de 2019.

UNIDAD REGULADORA DE CONTROL DE DATOS PERSONALES, URL: https://www.gub.uy/unidad-reguladora-control-datos-personales/?MOD=AJPERES&CONVERT_TO=url&CACHEID=c999a065-4daa-4d1b-8a68-%2520369139d60145 . Consultado el 20 de octubre de 2018.

UNIDAD REGULADORA DE SERVICIOS DE COMUNICACIONES: Informe de Mercado Telecomunicaciones, junio 2018. url: https://www.URSEC.gub.uy/inicio/transparencia/informacion-estadistica-y-de-mercado/telecomunicaciones/ Consultado el 9 de febrero de 2019.

UNIVERSITY OF CAMBRIDGE, URL: https://www.cipil.law.cam.ac.uk/sites/www.law.cam.ac.uk/files/images/www.cipil.law.

cam.ac.uk/documents/ipomodernisingipprofresponsepresspublishers.pdf Consultado el 20 de enero 2020.

YOUTUBE, https://youtube-creators.googleblog.com/2020/03/protecting-our-extended-workforce-and.html?m=1 Consultado el 13 de mayo de 2020.