GRADO EN COMERCIO

TRABAJO FIN DE GRADO

“CIBERSEGURIDAD Y PROTECCIÓN DE DATOS EN EL ENTORNO DIGITAL”

LARO GARCÍA SALVADOR

FACULTAD DE COMERCIO
VALLADOLID, NOVIEMBRE 2022

FACULTAD DE COMERCIO
Universidad de Valladolid

UNIVERSIDAD DE VALLADOLID
GRADO EN COMERCIO

CURSO ACADÉMICO 2021/2022

TRABAJO FIN DE GRADO

“CIBERSEGURIDAD Y PROTECIÓN DE DATOS EN EL ENTORNO DIGITAL”

Trabajo presentado por: Laro García Salvador

Tutor: Olatz Retortillo Atienza

FACULTAD DE COMERCIO

Valladolid, noviembre 2022

Agradecimientos a todos profesores que me han impartido clase durante la carrera, la cual considero la mejor del mundo.

A mis padres, Dani y Sonia, que gracias a ellos soy como soy y he conseguido llegar donde estoy.

A mi hermana pequeña, Jimena, que es capaz de sacarme una sonrisa en mis peores momentos.

A mi novia, Irene, que su apoyo diario supone para mí una bocanada de aire que me hace seguir adelante para conseguir mis objetivos.

Resumen

El fenómeno económico y social de la digitalización plantea tanto a las empresas como a los usuarios un entorno cada vez más complejo, confuso y con un mayor peligro ante los distintos retos y desafíos como consecuencia de cada vez estar más expuesto al exterior. A lo largo de este trabajo vamos a ver los efectos de este proceso que se reflejan tanto en el mercado como en la sociedad, así como las principales leyes creadas para regularización de este fenómeno con el fin de conseguir un mercado justo y competitivo.

Debido a esto, el desarrollo en las empresas debe de ir ligado al crecimiento en ciberseguridad y protección de datos de carácter personal, dos de los retos más importantes a los que se hace frente causado por el inexorable crecimiento de la digitalización a nivel mundial. Contar con métodos de actuación para diferentes situaciones puede ser lo que marque la diferencia entre afrontar un problema con la mayor brevedad posible o que la empresa desaparezca.

Abstract

The economic and social phenomenon of digitalization poses to both companies and users an increasingly complex, confusing and more dangerous environment in the face of the various challenges and challenges as a result of an environment that is increasingly exposed to the outside world. Throughout this paper we will see the effects of this process that are reflected both in the market and in society, as well as the main laws created to regulate this phenomenon in order to achieve a fair and competitive market.

Because of this, the development in companies must be linked to the growth in cybersecurity and protection of personal data, two of the most important challenges to be faced caused by the inexorable growth of digitization worldwide. Having methods of action for different situations can be what makes the difference between dealing with a problem as quickly as possible or the company disappearing.

ÍNDICE

ÍNDICE DE GRAFICAS

1. ANÁLISIS PRELIMINAR

En el primer apartado se realiza la descripción de contenidos y los temas a tratar en el trabajo, así como los objetivos perseguidos con el mismo, tanto a nivel general como a nivel específico. Igualmente, a continuación, se explica el método seguido para elaborarlo, la forma en la que se estructura y lo que ha llevado al autor a escoger este tema.

1.1. MOTIVACIÓN

Las principales razones que me han llevado a elegir este tema han sido dos. La primera de ellas es que se trata de un tema con una enorme amplitud y por tanto, de dificultad debido a la enorme cantidad de información que se obtiene en este entorno. Hay que recordar que la digitalización afecta al mercado en su integridad, generando una nueva estructura, a la que es necesario adaptar la legislación vigente, diseñada para un mercado tradicional. De este modo, a la novedad de la estructura digital, con nuevos retos y conflicto de intereses, se debe añadir las “viejas” cuestiones y problemas que se generan en la estructura tradicional, pero adaptándolas a la novedad de la digitalización

Por otro lado, la razón que tiene más peso para mí, es que se trata de un tema de constante actualidad, marcado por la tecnología y la innovación constante e imparable, así como su inevitable evolución dentro del mercado mundial, y por tanto, en comercio. Este crecimiento exponencial viene marcado por una cuestión de vital importancia: la ciberseguridad y la protección de los datos de carácter personal de todos los participantes y operadores en este mercado.

1.2. OBJETO

El objeto de estudio primordial de este Trabajo de Fin de Grado, en adelante TFG, es el análisis de la digitalización del mercado y el marco jurídico que lo ampara con el fin de conseguir un mercado justo y competente a todos los niveles. Además de esto, se valorarán los proyectos a nivel europeo y a nivel nacional desarrollados para impulsar la digitalización en las pequeñas y medianas empresas, así como planes de resolución a problemas que la digitalización conlleva.

Como colofón a este Trabajo de Fin de Grado se estudiarán posibles problemas a resolver dentro de los diferentes ámbitos que afectan al usuario/cliente de las plataformas digitales referidos a la protección de datos personales, seguridad electrónica, etc.

1.3. OBJETIVOS Y ALCANCE

Dada la extensión del contenido a la hora de abordar el mercado digital, se ha optado por centrarnos en dos temas relevantes del mismo. Por lo que el objetivo clave que se pretende conseguir con el análisis de este TFG es el de analizar la protección de datos de carácter personal y la seguridad electrónica en el medio digital.

Para poder alcanzar dicho objetivo, este TFG se subdividirá en los siguientes objetivos específicos:

- Estudiar la evolución histórica de la digitalización desde un punto de vista social y económico.
- Encuadre jurídico, tanto comunitario como nacional del mercado digital.
- Planteamiento de dos de las principales cuestiones que se plantean: la protección de datos y la ciberseguridad.

Lo que este análisis pretende lograr es ahondar en la importancia que tiene el fenómeno de la digitalización en cuanto a protección de datos a nivel personal y seguridad electrónica. El estudio que se llevará a cabo será sobre un suceso continuo y real en el tiempo, lo que nos dará un punto de vista de cómo la digitalización afecta en el día a día del mercado y nos permitirá descubrir los nuevos peligros que vienen del fenómeno de la digitalización.

1.4. METODOLOGÍA

La metodología usada en este trabajo será el acceso a la normativa y bases de datos de carácter oficial y otras webs de interés en materia de seguridad y protección de datos, tanto a nivel nacional como comunitario, pues es lo que nos va a dar el encuadre de la realidad económica y social en la que incide. Además, se utilizará tanto comentarios académicos como impresiones periodísticas y noticias de divulgación sobre los temas de actualidad que incidan directamente en el tema a tratar.

En la segunda parte del trabajo se estudiará los métodos utilizados por la Unión Europea y por el Gobierno de España para abordar el fenómeno de la digitalización y los principales problemas planteados. Para ello se ha accedido a distintos recursos de información públicos como pueden ser la página web Noticias del Parlamento Europeo o la web de la Moncloa en el caso nacional.

1.5. ESTRUCTURA

En primer lugar, la introducción, que se encargará de ponernos en contexto de lo que significa realmente la digitalización y la relación que tiene directamente con el mercado. De igual manera se explicará la evolución de este fenómeno.

- A continuación, se mostrarán las ventajas y desventajas tanto económicas como sociales y las soluciones que diferentes organismos han impuesto como resoluciones a este problema.

- En el siguiente apartado se explicarán las diferentes leyes y normas creadas para conseguir un mercado competente y con igualdad de oportunidades. Además, en este apartado también se expondrán diferentes proyectos europeos y nacionales para lograr el objetivo mencionado anteriormente.

- Seguidamente se valorarán los problemas y cuestiones a resolver que esta revolución tecnológica ha generado.

- Finalmente se proporcionarán una serie de conclusiones que plasmará la veracidad y seguridad de la digitalización en el mercado y si las leyes que ampara este "nuevo" fenómeno son fiables.

2. INTRODUCIÓN

En este primer bloque se presentará una breve descripción de lo que es la digitalización y el modo en el que afecta al mercado y a nuestras vidas. Así como su historia desde los primeros pasos hasta día de hoy y la repercusión en la economía y sociedad.

Vivimos en un mundo donde la globalización y la necesidad de estar conectados es clave para un desarrollo futuro. Para ponernos en situación, en abril de este año había alrededor de 7 930 millones de personas en nuestro planeta de las cuales, según *'Digital*

2022 April Global Statshot', 5 000 millones utilizan Internet[1] (esto supone un 63% del global), 200 millones de personas más que el año pasado.

2.1. Concepto y breve historia de la digitalización

La digitalización es un fenómeno social, cultural y empresarial, no es una cosa únicamente tecnológica, aunque evidentemente la tecnología tiene mucho que ver. Lo que está cambiando con la digitalización son las personas y la manera en cómo compran, se comunican, comparten y colaboran. La digitalización es el proceso fenomenal con el que la empresa utilizan las tecnologías de la información para vender mejor, para llegar mejor a los clientes, para entender mejor sus necesidades y para adelantar los comportamientos, es decir, cómo usar las tecnologías para funcionar mejor.

En primer lugar, hay que establecer en qué consiste la digitalización de una empresa, para ello es necesario destacar que desde la Revolución Industrial las compañías han competido entre sí con sus capacidades para desarrollar y adoptar tecnologías con el propósito de reducir los costes y aumentar la productividad, dos factores muy determinantes. En el siglo XXI estamos contemplando como las TIC, es decir, las tecnologías de la información y la comunicación, se están convirtiendo en estrategias para compañías no digitales. Negocios con establecimientos físicos se están digitalizando, fomentando nuevos modelos como por ejemplo el autoservicio, este fenómeno está cambiando la forma en la que funciona el mercado. Las empresas están asimilando la necesidad de innovar de manera sistemática usando para ello tecnología,

a riesgo de caer frente a un competidor más entusiasta e imaginativo en el uso de tecnologías digitales.

Si bien consideramos el uso de la tecnología como algo indispensable en la actualidad dentro de nuestro día a día, hay que tener en cuenta que, de un tiempo a esta parte, este proceso ha constituido una transformación total en nuestra forma de entender la vida. El proceso de digitalización global que estamos viviendo en la actualidad viene dado por una sucesión de avances, desarrollos y progresos tecnológicos los cuales han supuesto mejoras y comodidades en la mayoría de las acciones que realizamos cada día. Desde

[1] https://wearesocial.com/es/blog/2022/04/mas-de-5-mil-millones-de-personas-ya-usan-internet/

hace unos años, la transformación digital[2] ha pasado de ser una simple elección la cual podías tomar a ser algo prácticamente imprescindible para poder vivir.

La digitalización como suceso produce una serie de cambios en todos los aspectos fundamentales de la vida tal y como los conocíamos hasta entonces. Este proceso contribuye no solo a la mejora de estos aspectos, sino que también a la facilidad de su desarrollo. Tales cuestiones abarcan desde lo más simple, como puede ser la comunicación humana (con la aparición del correo electrónico en 1971), hasta lo más complejo como puede ser la involucración de la inteligencia artificial en el proceso productivo de algunas empresas (Industria 4.0).

Pero esto no fue siempre así, la electrónica no es algo nuevo ni mucho menos, su nacimiento data de 1703 con el desarrollo de un sistema de números de base 2 conocido como sistema binario, posteriormente, esta explicación de la aritmética binaria sería concebido como el principio de la digitalización. El fenómeno del que estamos hablando lleva consigo una aceleración vertiginosa de la innovación tecnológica que conduce a un ritmo de cambio y adaptación continuo que, como he mencionado antes, se vuelve inevitable y totalmente necesario para la vida diaria de una persona o empresa.

La transformación digital es un hecho irreversible que ha cambiado el mundo tal como lo conocemos y entendemos, afectando a todos los aspectos de nuestras vidas tanto a nivel económico como a nivel cultural, social y político. Internet se creó en el año 1969 como una red de comunicación entre cuatro universidades de Estados Unidos, pero no fue hasta el principio de la década de los 90 que surgió la WWW (World Wide Web)[3], su transición de un entorno puramente corporativo/universitario a convertirse eventualmente en una red de redes

Con la introducción de la World Wide Web, el alcance, la dimensión, la escala, la velocidad y la eficiencia de la digitalización han cambiado significativamente, ejerciendo más presión sobre el proceso de transformación social. Estadísticamente, en la última década del milenio, el número de usuarios pasó de unos cientos de miles a 350 millones; En la primera década del siglo XXI, el número de usuarios conectados a Internet aumentó de 350 millones a 2 mil millones.

[2] Transformación digital: La transformación digital es la integración de las tecnologías digitales en las empresas y su impacto en la sociedad. https://www.europarl.europa.eu/news/es/headlines/priorities/transformacion-digital/20210414STO02010/transformacion-digital-importancia-beneficios-y-politicas-europeas

[3] WWW World Wide Web: es un sistema que funciona a través de Internet, por el cual se pueden transmitir diversos tipos de datos a través del Protocolo de Transferencia de Hipertextos o HTTP, que son los enlaces de la página web.

Internet es conocida también como la “red de redes” y en ella participan desde grandes sistemas hasta computadoras personales. En Internet se ponen a disposición de los millones de usuarios tanto instituciones oficiales como gubernamentales como educativas, científicas y empresariales. A esta red se fueron uniendo países de Europa y de todo el mundo para acabar formando la WWW.

2.2. Digitalización del mercado y mercado tradicional

Hablamos de comercio tradicional cuando se realiza una transacción de compra-venta bienes en una tienda física cara a cara, es decir, de forma presencial e intercambiando bienes por dinero. En cambio, en el comercio electrónico, estas transacciones se realizan a través de internet, sin necesidad de estar cara a cara.

La evolución y el aumento del desarrollo del comercio electrónico ha transformado totalmente el modo en que trabajan las empresas a día de hoy. La utilización de este tipo de comercio en detrimento del tradicional no es una simple casualidad, viene dado por una serie de diferencias clave que ha empezado a atraer a un número de compradores cada vez más elevado.

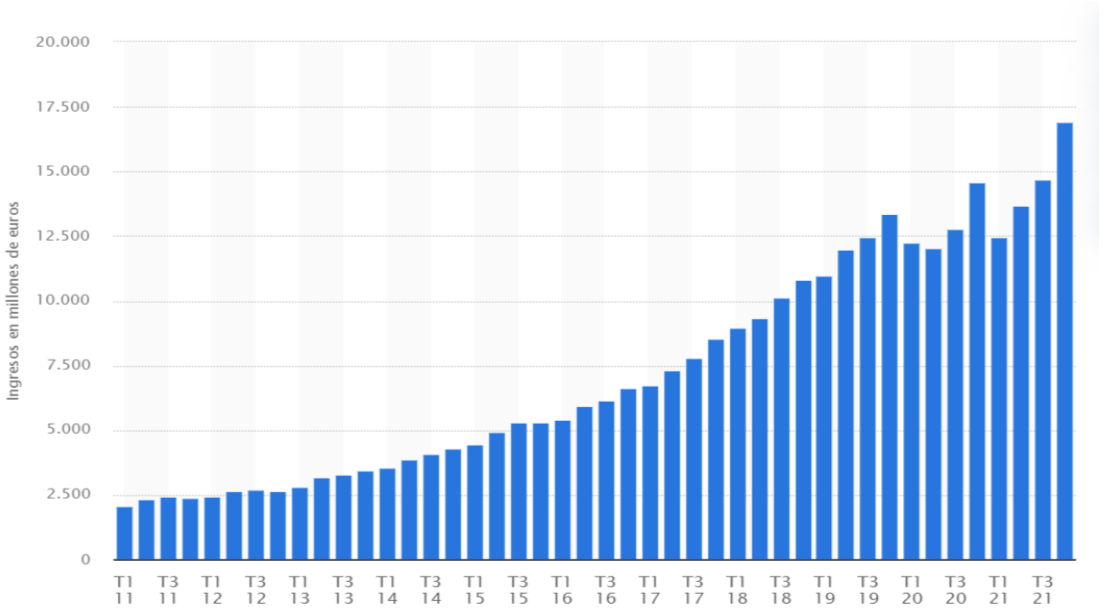
La mayoría de los consumidores que realizan sus compras de manera on-line lo hacen por una serie de razones entre las cuales están:

- La comodidad: mediante el comercio electrónico no es necesario que salgas de casa para hacer una compra, de la otra forma tendrías que salir a la calle para realizar la transacción.
- Ofertas: otra razón por la que los clientes prefieren las plataformas on-line es porque encuentran más ofertas, promociones o descuentos (por ejemplo, muchas de las tiendas que venden a través de internet te ofrecen un determinado descuento por registrarte en su página web).
- Variedad de productos: en las tiendas físicas, el número de productos que tienen a la venta está limitado por el espacio de la misma, mientras que en la web de esa misma tienda puedes disponer de todos los productos del catálogo.
- Horarios de compra: a la hora de realizar una compra de forma on-line puede ser ejecutada a cualquier hora del día, en cambio si se hace en una tienda

física debe de ser dentro del horario de apertura de la tienda, lo cual supone una desventaja.

A lo largo de estos últimos años, el *e-commerce* ha sufrido un gran aumento debido al incremento del acceso a Internet a nivel mundial y al proporcionar productos o servicios personalizados.

Gráfico 1 Volumen total de negocio por comercio electrónico en España desde el tercer trimestre de 2011 al cuarto trimestre de 2021. En millones de euros.



Fuente: Statista[4]

Entre los meses de octubre y diciembre del año pasado, el *e-commerce* en España obtuvo un volumen de negocio de cerca de 16.916 millones de euros. Esta cifra supuso un aumento de más de 2.200 millones de euros respecto a la facturación del trimestre anterior. Esta gráfica está elaborada a partir de los datos obtenidos por medio de un estudio realizado por la Comisión Nacional de los Mercados y la Competencia (CNMC)

El *e-commerce* ha constituido una revolución a nivel mundial respecto a las transacciones comerciales. En nuestro país, cerca del 23%[5] del total de las compras se llevaron a cabo a través de Internet en 2020. A decir verdad, en el último trimestre de 2020,

[4] https://es.statista.com/estadisticas/496407/ingresos-por-ventas-en-el-comercio-electronico-en-espana/#:~:text=Facturaci%C3%B3n%20total%20del%20ecommerce%20por%20trimestre%20en%20Espa%C3%B1a%20T1%202011%2DT4%202021&text=Entre%20octubre%20y%20diciembre%20de,aproximadamente%2016.916%20millones%20de%20euros

[5] https://www.cnmc.es/prensa/ecommerce-4T20-20210702

la facturación proveniente del comercio on-line logró alcanzar un máximo histórico al sobrepasar los 14,5 millones de euros dentro del territorio.

En cambio, las tiendas físicas cada vez tienen menos presencia y relevancia sobre todo las empresas de moda, ocio, calzado y complementos, viajes… las cuales a través de un simple clic puedes comprar sus productos o servicios sin necesidad de acudir a una tienda física.

2.3. Encuadre de la realidad económica y social

Como he mencionado antes, el fenómeno de la digitalización abarca muchos ámbitos de nuestra vida, tanto personal y socialmente como profesionalmente, pero no solo esto afecta a las personas, sino que también al mercado y al ámbito comercial. Desde hace unos años la evolución de las empresas y la necesidad de adaptarse al emergente estilo de negocio a través de la digitalización de las mismas ha seguido una pendiente ascendente continua. Las nuevas formas de acercar el producto al cliente o de producir los bienes y servicios se han impuesto ante la tradicional forma de hacer negocios. Los avances tecnológicos cada vez son más y mejores, además de suponer en la mayoría de los casos un coste menor para las empresas, estos facilitan los procesos que se han de realizar dentro de una empresa.

Otros puntos de vista sin salirnos del ámbito comercial es el de los nuevos medios de pago (PayPal, Wallets digitales, Bizum, Criptomonedas…) o bien el de la presencia de Inteligencia Artificial en el proceso productivo de las empresas (robots en el proceso de montaje en los sectores de la automoción, la máquina de riego en el sector agrario o los drones mensajeros ya introducidos en algunas empresas).

Desde el punto de vista de la empresa, las compañías digitales necesitan empleados capaces de incorporar y gestionar las tecnologías. Los grados tecnológicos, especialmente los conocimientos relacionados con la tecnología avanzada y la inteligencia artificial van a experimentar un fuerte impulso y, por otro lado, en paralelo, las organizaciones digitales necesitan profesionales para la colaboración, el trabajo en equipo, la empatía con el cliente y la comunicación.

Por otro lado, otros de los grandes cambios en la automatización externa de los procesos, con el desarrollo de las nuevas tecnologías inteligencia artificial, procesos que se habían resistido la automatización pasarán a realizarse sin intervención humana. Los

centros de atención al usuario o algunas tareas diagnósticas son claros candidatos a ser realizados digitalmente y con ello se reducirá la necesidad de contratar personal o en su caso se producirá una sustitución de los puestos de trabajo empleados en determinadas tareas ya que ahora se llevarán a cabo digitalmente.

A continuación, vamos a hablar sobre la adaptación de los trabajadores a la empresa digitalizada. En primer lugar, es importante mencionar que, gracias a la digitalización, cada vez se están automatizando más tareas y procesos, y esta tendencia seguirá en aumento. La transformación digital está facilitando que se mejore la productividad de las empresas principalmente consiguiendo reducir errores y permitiendo un control y seguimiento más exhaustivo de los procesos.

La automatización de los procesos y las tareas de las empresas gracias a la digitalización generan en muchas ocasiones cierto rechazo o resistencia a introducir nuevas tecnologías al trabajo diario, tanto en la inversión económica empresarial necesaria, como por la incertidumbre sobre cómo afectará a los a los actuales puestos de trabajo. Conseguir que la digitalización sea una realidad en las empresas no depende únicamente de la inversión en tecnología e innovación sino de que las personas sean agentes de cambio en su propio proceso hacia la digitalización y tengan las actitudes, habilidades y competencias digitales necesarias para ello.

Asimismo gran parte de la actividad realizada hoy por profesionales en las empresas, es decir, la mano de obra, va a ser desempeñada mediante inteligencia artificial, lo que producirá que gran parte de los trabajadores de las empresas y el proceso de digitalización sean sustituidos por el uso de dispositivos o de robótica avanzada o que estos empleados pueden experimentar cambios en sus funciones y tareas lo que conlleva un proceso de adaptación a un nuevo método de trabajo, es decir, van a desaparecer ciertos puestos de trabajo pero también aparecerán otros. Esto provoca que muchas personas tengan la sensación de sentirse amenazados por estas nuevas demandas, por ello se trata de un elemento sobre el que actuar por parte de la empresa y también por parte de los trabajadores.

Siguiendo con lo planteado la digitalización creará empleo de calidad, se conseguirá que tareas repetitivas y rutinarias se puedan realizar con mayor rapidez y conectividad evitando duplicidades o procesos improductivos. Por todo ello es necesario un apropiado acompañamiento de sensibilización, formación y para que se puedan llevar a cabo adecuaciones en los puestos de trabajo e iniciar la ruta hacia la transformación digital. Cabe

destacar también que la gestión de personas siempre ha sido un reto y ante la resistencia al cambio las empresas tienen nuevos elementos a los que hacer frente.

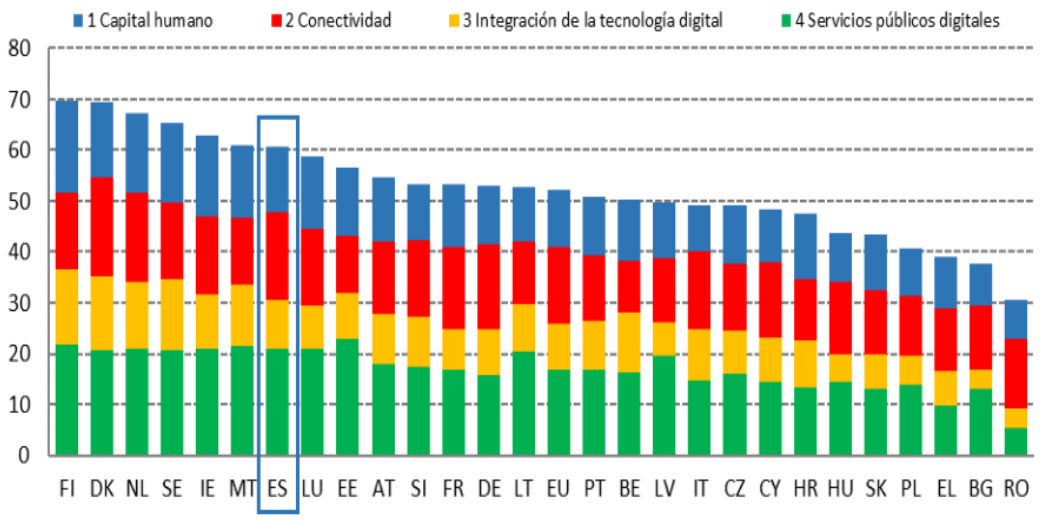
3. Efectos de la digitalización

3.1. Evolución económica y social

La correcta evolución del mercado de trabajo a causa de la digitalización radica principalmente en la continua formación de los trabajadores para tener un futuro laboral próspero. Una de las principales consecuencias de la digitalización de las empresas no es el reemplazo de los trabajadores por máquinas, como estamos acostumbrados erróneamente a oír, sino que lo que realmente cambiará es la naturaleza del trabajo. Explicado con un ejemplo, esto significa que, una empresa que se dedica al montaje de vehículos se mecaniza y la cadena de montaje pasa a estar formada por máquinas, en vez de por trabajadores. Lo que la empresa pretende es que los mismos trabajadores que estaban en la cadena de montaje sean los que hagan funcionar esas máquinas y los que las reparen en caso de avería. Esto se denomina *reskilling*, comúnmente conocido como reciclaje profesional, busca formar a un empleado con el objetivo de ubicarlo en un nuevo puesto dentro de la organización.

Otra estrategia de formación dentro de las empresas es el *upskilling* cuyo objetivo es mostrar a un trabajador nuevas competencias para hacer su trabajo más efectivo y eficiente. Estas dos estrategias tienen objetivos beneficiosos para las empresas, como son: el combatir la brecha digital, promover una cultura de empresa dinámica que está adaptada a un entorno en constante evolución, ayudan a crear fidelidad a la empresa y a retener talento…

Gráfico 2: Índice de la Economía y la Sociedad Digitales. Año 2022



Fuente: Portal web de Comisión Europea. Sitio web oficial de la UE.[6]

Para comenzar, el Índice de la Economía y la Sociedad Digitales (DESI) lo que hace es definir los indicadores sobre el rendimiento digital de Europa y seguir el avance de los países de la UE.

Los informes DESI 2022[7] se basan esencialmente en datos de 2021 e investigan la mejora digital realizado en los Estados miembros de la UE. Durante la pandemia de COVID-19, los Estados miembros han prosperado en sus esfuerzos de digitalización, pero aún insisten en cerrar las brechas existentes en las habilidades digitales, la transformación digital de las pymes y el despliegue de redes 5G avanzadas.

Nuestro país ocupa el puesto número 7[8] de los 27 Estados miembros de la UE en la edición de 2022 del Índice de la Economía y la Sociedad Digitales (DESI). El país está logrando un progreso relativo1 y mejorando sus resultados en comparación con años anteriores, sobre todo en lo que se refiere a la integración de la tecnología digital (puesto número 11, cinco puestos mejor que en 2021), así como en los servicios digitales públicos (puesto número 5 en comparación con el puesto número 7 de 2021) y en términos de capital humano (puesto número 10 en comparación con el puesto número 12). España es uno de

[6] https://cde.ugr.es/index.php/union-europea/noticias-ue/1427-indice-de-la-economia-y-la-sociedad-digitales-2022-espana-alcanza-el-septimo-puesto
[7] https://administracionelectronica.gob.es/pae_Home/pae_OBSAE/Posicionamiento-Internacional/Comision_Europea_OBSAE/Indice-de-Economia-y-Sociedad-Digital-DESI-.html
[8] https://www.lamoncloa.gob.es/serviciosdeprensa/notasprensa/asuntos-economicos/Paginas/2022/280722-digitalizacion.aspx

los líderes de la UE en cuanto a conectividad y ocupa el puesto número 3 por segundo año consecutivo.

3.2. Ventajas e inconvenientes de la digitalización

Todos estos cambios y avances hacen que nos cuestionemos las ventajas y desventajas que tiene este proceso. En España algunos de los datos son bastante reveladores. Cuando hablamos de la digitalización del mercado una de las primeras cosas que se nos viene a la mente es el comercio electrónico. El *e-commerce* (comercio electrónico) "se refiere generalmente a todas las formas de transacciones relacionadas con las actividades comerciales, incluyendo organizaciones e individuos, que están basadas en el proceso y transmisión de datos digitalizados, incluyendo texto, sonido e imagen"[9] ha sido durante años una herramienta muy poco utilizada por los compradores en nuestro país, no obstante, con el paso del tiempo España ha logrado ser uno de los países que más evolución ha experimentado respecto a las compras por Internet. El *e-commerce* cuenta con varias ventajas sobre el comercio tradicional entre las cuales se encuentran: la posibilidad de no contar con ninguna restricción horaria, es decir, está abierto las 24 horas; la comodidad para el cliente a la hora de comprar, ya que puede adquirir los productos desde cualquier lugar y hora; cuenta con unos costes más bajos ya que se reducen los asociados con la comercialización, gestión de inventarios, atención al cliente…

La llegada de Internet a España se produce en 1990, fue algo muy innovador y revolucionario, pero hasta el comienzo del nuevo milenio no se empezaron a ver cifras muy representativas que digamos. Durante el año 2001, la facturación del *e-commerce* fue de 525,12 millones de euros[10], lo que supuso un 157 por ciento más que la campaña anterior, además durante este año solo el 6,5 por ciento de las empresas españolas realizaron ventas por Internet. DATO DE LA Asociación Española de Comercio Electrónico. Desde entonces, el comercio electrónico B2C[11] (acrónimo en inglés de "business to consumer") en España ha sufrido una tendencia de crecimiento continuo durante los últimos 20 años.

---

[9] Davis, C, Hajnal, C, DeMatteis, D. y Henderson, M, Requerimientos de Administración de Recursos para Comercio Electrónico (reporte preparado para Industria Canadá, 1998).

[10] https://www.lavanguardia.com/tecnologia/20020424/51262753522/el-e-commerce-espanol-facturo-525-millones-en-2001.html

[11] B2C: es un tipo de práctica existente en el ámbito del marketing. Habitualmente, es empleada por firmas comerciales que persiguen llegar de manera directa a un cliente o consumidor final. https://economipedia.com/definiciones/business-to-consumer-b2c.html

Los datos registrados en 2020 lo confirmaron. En ese año, las ventas online de la empresa a los consumidores españoles generaron unos ingresos superiores a los 50.000 millones de euros. Eludiendo los beneficiosos datos económicos, otras ventajas con las que cuenta la transformación digital la de agilizar los procesos y operaciones de las organizaciones para que estas logren alcanzar sus metas de manera más rápida.

Pero es cierto que no todo son ventajas dentro del amplio campo de la digitalización del mercado. Este proceso requiere una inversión la cual todas las empresas no pueden asumir, muchos de los nuevos avances tecnológicos son altamente costosos por lo que muchas empresas se ven obligadas a prescindir de ellos lo que a su vez provoca notables diferencias entre distintas compañías y aumenta su competitividad. Otra de las grandes desventajas de esta transición tecnológica es que los progresos parecen no tener fin, estos avances se están renovando casi a diario, de manera que, lo que hace un año parecía el adelanto tecnológico definitivo, a día de hoy puede resultar obsoleto e inútil frente al nuevo sustituto. Además, la captación de personal cualificado puede resultar un proceso prolongado en el tiempo o bien los trabajadores de la empresa pueden ofrecer resistencia a los cambios organizativos que quiera implementar la propia organización.

Para terminar este apartado es significativo señalar dos de los más importantes problemas que la digitalización trae consigo: la protección de datos personales y la ciberseguridad. Estos dos puntos serán desarrollados en la última parte del trabajo.

4. ENTORNO COMUNITARIO PARA ABORDAR LA DIGITALIZACIÓN

4.1. Proyectos europeos

Para que los impactos de estas desventajas no sean tan abrumadores, la Unión Europea ha lanzado dos programas de ayudas que supondrán el inicio de un proceso de digitalización a nivel de toda la Unión Europea nunca antes visto. Consta de dos Planes de Recuperación que contribuirán a reparar los daños económicos y sociales causados por la pandemia. Está orientado tanto a Pymes como a grandes Empresas.

El primero de estos proyectos europeos es el denominado Next Generation, un fondo masivo de recuperación que cuenta con más de 800 mil millones de euros (el 5% del PIB de la UE) y que entró en vigor el 21 de julio de 2020 gracias al Consejo Europeo

después de cuatro días de negociaciones. Este proyecto cuenta con un elemento central denominado Mecanismo de Recuperación y Resiliencia (MRR).

El Mecanismo de Recuperación y Resiliencia, con su entrada en vigor el 19 de febrero de 2021, tiene como finalidad principal aplacar el impacto social y económico consecuencia de la pandemia coronavirus y conseguir que las comunidades europeas sean más sostenibles y resilientes, así como para lograr que estén preparadas para los desafíos de la transición digital. Dentro del programa NextGenerationUE, el MRR presenta una oportunidad sin antecedentes para impulsar la transformación digital con un presupuesto de 672 500 millones de euros[12]. Este capital invertido se divide en 360 000 millones destinados a en forma de préstamos y 312 500 millones de euros en forma de subvenciones. El MRR financiará las reformas e inversiones que se realicen en los Estados Miembros con fecha de fin el 31 de diciembre de 2026.

Además del RMM existen otros programas como Ayuda a la Recuperación para la Cohesión y lo Territorios de Europa (REACT-UE) que ayudará a una recuperación digital, ecológica y resiliente de la economía. Y otros programas como Horizonte 2020, Desarrollo Rural o Fondo de Transición Justa.

Por último, cabe destacar que España es el País Miembro que más dinero ha recibido hasta el momento con un total de 77 234 071[13] de euros.

El segundo de los proyectos es el denominado Programa Europa Digital 2021-2027, el cual tiene como principal objetivo crear una herramienta de gasto para promover y maximizar las ganancias de esta transformación digital para las organizaciones y administraciones públicas de la Unión Europea a través del perfeccionamiento de las capacidades digitales en cinco sectores que resultan claves. Estos sectores son los siguientes: la informática de alto rendimiento[14], la Inteligencia Artificial (IA), la Ciber Seguridad y Confianza, el Despliegue y Habilidades Digitales Avanzadas y un mejor uso de las Capacidades Digitales e Interoperabilidad.

El Programa Europa Digital[15] es un programa de inversión, que contará con un capital de 7 600 millones de euros, que servirá para fortalecer las capacidades digitales estratégicas de la UE y contribuir a promover el despliegue a gran escala de tecnologías

[12] https://www.hacienda.gob.es/es-ES/CDI/Paginas/FondosEuropeos/Fondos-relacionados-COVID/MRR.aspx
[13] https://www.lamoncloa.gob.es/presidente/actividades/Documents/2020/07102020_PreguntasRespuestasPR.pdf
[14] La informática de alto rendimiento (HPC) es el uso de tecnología informática avanzada, como supercomputadoras y algoritmos de procesamiento paralelo, para resolver problemas informáticos complejos. https://spiegato.com/es/que-es-la-informatica-de-alto-rendimiento
[15] https://ec.europa.eu/info/funding-tenders/find-funding/eu-funding-programmes/digital-europe-programme_es

digitales para su posterior utilización por parte los ciudadanos y las empresas europeas. Incluye, del mismo modo, las prioridades fundamentales de la UE en estos momentos, a saber: una transición verde y digital y la adaptabilidad del mercado único. El programa incluye el requisito de que ningún estado miembro de la UE pueda, por sí solo, llegar a alcanzar el grado de éxito digital solicitado.

Por último, los criterios éticos se han de tener en cuenta cuando se desempeñen actividades en las que estén implicadas la Inteligencia Artificial. El importe global de este programa asciende a siete mil quinientos ochenta y ocho millones de euros para el período 2021-2027. Todo este importe tiene la posibilidad de cubrir hasta el 100% de los costes subvenciónales.

4.2. Iniciativa nacional

Además de estos dos proyectos a nivel europeo, el Gobierno de España ha implantado un nuevo plan denominado “España digital 2026”[16]. Dentro de este plan se proponen diferentes estrategias como el despliegue de redes y servicios para mejorar la conectividad digital, el perfeccionamiento de la Administración digital, la formación en competencias digitales y la digitalización de la economía. Nuestro país cuenta con una de las mejores redes de infraestructuras digitales a nivel mundial, organizaciones líderes en los sectores punteros como son el de la salud, la alimentación agraria, la movilidad o el turismo, o las finanzas. Además de esto la sociedad española es una sociedad diversa, dinámica y ágil adaptándose al cambio.

El primero de los proyectos está financiado a través de los fondos Next Generation EU para la digitalización de las pymes y autónomos de nuestro país. Se denomina Kit Digital y éste consiste fundamentalmente en un programa de ayudas económicas del Ministerio de Asuntos Económicos y Transformación Digital que ayuda a impulsar el cambio digital en las empresas que lo soliciten para así hacer que se involucren en el mercado de una manera más competitiva.

Este proyecto cuenta con un presupuesto de 3.067 millones de euros, de los cuales 500 millones se destinarán a las pymes de entre 10 y 49 trabajadores y los 2.500 millones restantes irán destinados a microempresas y autónomos. De esta manera, cada perfil

[16] https://portal.mineco.gob.es/es-es/ministerio/estrategias/Paginas/00_Espana_Digital.aspx

contará con una cuantía de subvención fijo que dependerá del volumen de la empresa, la complejidad del paquete, el sector de actividad y demás condiciones.

España también se encuentra en una posición relativamente buena en la digitalización de la gestión y tiene un gran potencial en la implantación de las tecnologías más modernas para la gestión de la información y la puesta en funcionamiento de políticas públicas. Pero, por otro lado, los avances han sido más escasos en otros ámbitos como los de la transformación digital en la industria y la empresa, en particular PYMES, I+D+i, y de la preparación y formación de la población española. Estas tres, resultan claves para que la transformación digital del país sea completamente satisfactoria, sin olvidar otras áreas como el ámbito rural o las brechas sociales y territoriales existentes.

El Ministerio de Asuntos Económicos y Transformación Digital, por medio de la Secretaría de Estado de Digitalización e Inteligencia Artificial, invita públicamente a las CC.AA. a colaborar en la nueva idea de la Agenda España Digital 2026: 'RETECH: Redes territoriales de especialización tecnológica'.

La finalidad de este segundo programa es el de mejorar la co-gobernanza del Plan de Recuperación por medio de proyectos regionales encaminados al cambio y la especialización digital. El apoyo a estos planes impulsará el tráfico de conocimiento y las oportunidades de cada comunidad autónoma por medio de redes de repercusión nacional que posibiliten la maximización del equilibrio en el territorio y la cohesión social.

El Gobierno va a destinar al proyecto RETECH[17] 530 millones de euros del Plan de Recuperación durante el periodo 2022-2023, que contará con inversión adicional de las comunidades autónomas. Gracias a esta inversión se darán comienzo a planes con un impacto muy elevado en el ámbito territorial y más concretamente en el sector de la Inteligencia Artificial. Estos proyectos son: los Gemelos Digitales como las soluciones tecnológicas de simulación virtual de objetos y sistemas; las tecnologías "verdes por diseño" (GreenTech), la Ciberseguridad, las Redes de Emprendimiento Digital, la digitalización en entornos rurales y despoblados (RuralTech), la industria de la moda y el textil (FashionTech) y la Salud Digital.

[17] https://portal.mineco.gob.es/es-es/comunicacion/Paginas/retech.aspxm

4.3. Impacto de la Covid-19 en la evolución de la digitalización

Pero no solo se consigue el progreso por medio de programas o proyectos financiados como los que acabo de mencionar. Uno de los factores clave para que la transformación digital haya avanzado a pasos agigantados durante estos dos últimos años ha sido la aparición de la pandemia global Covid-19, la cual provocó la puesta en cuarentena y aislamiento de la población mundial durante un período medio de 2 meses, como consecuencia de esto muchas empresas se vieron obligadas a cerrar sus negocios durante este período de tiempo y finalmente se vieron obligadas a cerrar. Muchas otras empresas, en general las organizaciones digitalizadas, se vieron favorecidas como son el caso de las tiendas de comercio electrónico como Amazon, EBay y Jd.com entre otras. De lo que no cabe duda es que la pandemia fue la causante de que se haya producido un avance que, quizás, en una situación de normalidad hubiera requerido años, por lo que podemos afirmar con total seguridad la ventaja que el Covid-19 ha supuesto para el desarrollo de una digitalización global. No en vano, en 2020 se registró el mayor número de transacciones de comercio electrónico hasta la fecha. El continuo incremento del volumen de negocio del *e-commerce* B2C en nuestro país es clara evidencia de que cada vez es más elevado en número consumidores que deciden realizar sus compras en las tiendas online.

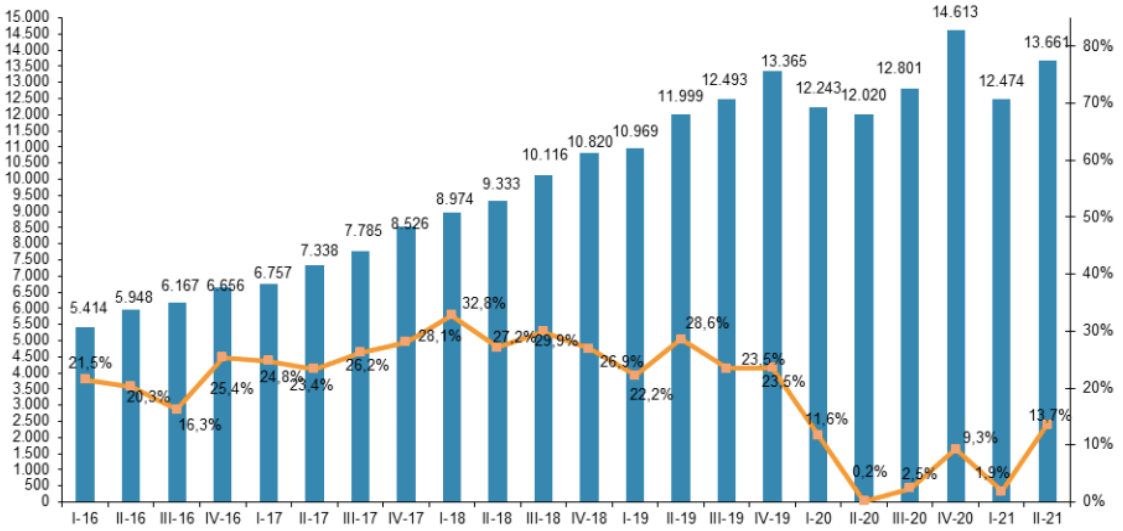
Durante la época de la pandemia en Europa la mitad de los trabajadores llegaron a desempeñar sus empleos de manera telemática, la venta presencial al por menor se vio superada por el *e-commerce,* el cual creció más de un 20%[18] y los pagos en papel o moneda fueron sustituidos por el pago por medios digitales en muchos comercios y servicios. El *e-commerce* Según la opinión de la presidenta del Banco Central Europeo, Christine Largade, estos cambios tan drásticos en los nuevos modos que trabajamos compramos o pagamos se van a volver permanentes. También se presiente la llegada, a través de esta digitalización, una globalización basada en los servicios en la web, como por ejemplo las visitas médicas, algo que ya está en uso.

Sin duda alguna el *e-commerce* ha llegado en nuestro país para quedarse, y esto se corrobora observando los últimos datos que publicó la Comisión Nacional de los Mercados y la Competencia (CNMC), los cuales establecen que el comercio electrónico en España ha sobrepasado lo 13 600 millones de euros en el segundo trimestre de 2021, lo

[18] https://ecommercerentable.es/ecommerce-espana-2021/#:~:text=El%202020%20el%20ecommerce%20en,de%20forma%20importante%20y%20consolidandose.

que se traduce en un 13,7% más de los alcanzado el año anterior[19]. El siguiente gráfico representa la evolución trimestral del volumen de negocio del comercio electrónico y variación interanual.

Gráfico 3 Evolución trimestral del volumen de negocio del comercio electrónico y variación interanual



Fuente: CNMC[20]

Dicho esto, los beneficios que nos proporciona la digitalización parecen claros, sin embargo, algunas de las organizaciones que cuentan con mayores ventajas en este campo tienen una superioridad excesiva sobre las empresas competidoras. Para evitar que esta situación derive en irrefrenable, la Comisión Europea, ha desarrollado una serie de leyes que proporcionarán más estabilidad, justicia y ética a todo el entorno de la digitalización en las organizaciones. Una de ellas en la Ley de Mercados Digitales, la cual tratará de igualar la situación y las oportunidades de todas las empresas digitales, sea cual sea su tamaño, para así terminar con la mala praxis sobre organizaciones y consumidores. Esta nueva Ley de Mercados Digitales establecerá las normas sobre lo que las grandes plataformas digitales[21] podrán hacer, o no, dentro de la Unión Europea.

[19] https://www.cnmc.es/prensa/comercio-electronico-iit-2021-20220107
[20] https://es.statista.com/estadisticas/496407/ingresos-por-ventas-en-el-comercio-electronico-en-espana/
[21] Las plataformas digitales son infraestructuras digitales que permiten que dos o más grupos interactúen. Por lo tanto, se posicionan como intermediarios que reúnen a diferentes usuarios: clientes, anunciantes, proveedores de servicios, productores, proveedores e incluso objetos físicos. Nick Srnicek, Capitalismo de plataformas (2017).

El mundo digital tiene cada vez más relevancia en nuestras vidas y hay muchos puntos que no están correctamente normalizados todavía. Esto da a entender que uno de los mayores retos, sino el que más, que debe de afrontar la economía digital no atañe a las evoluciones tecnológicas, sino a los avances jurídicos que tienen que garantizar un entorno justo, digno y favorable a la aparición de nuevos tipos de negocio.

5. Leyes reguladoras de la digitalización

5.1. Ley de Mercados Digitales

La Propuesta de Reglamento del Parlamento Europeo y del Consejo sobre mercados disputables y equitativos en el sector digital conocida como Ley de Mercados Digitales[22] es una normativa orientada a los servicios de mensajería, a la publicidad en línea y en general a las prácticas llevadas a cabo por la las plataformas tecnológicas más grandes. Esta Ley de Mercados Digitales implanta una serie de normas que se aplican a las plataformas digitales que ejerzan de "guardianes de acceso" en el sector digital. Estas plataformas, que poseen una posición aventajada y prolongada en el tiempo, tienen una repercusión notable en el mercado interior y ejercen como conducto para comunicar a los usuarios profesionales con los usuarios finales. Es decir, que actúan como mediadores entre las empresas y los usuarios finales.

Esta ley tiene como principal objetivo el de evitar que estos "guardianes de acceso" implanten una serie de condiciones abusivas tanto para las empresas como para los usuarios finales y proteger la libre utilización de los servicios digitales más importantes. Estas plataformas protectoras de la igualdad de oportunidades en el mercado digital deberán garantizar, entre otras cosas, la seguridad de los usuarios a la hora de dar de baja su suscripción fácilmente a los servicios de la plataforma en cuestión, suspender la puesta en marcha de un programa informático junto con el sistema operativo por posibles defectos, acceder a que los desarrolladores puedan utilizar sistemas de pago alternativos a los integrados en la aplicación, facilitar las cifras de rentabilidad publicitaria… unas directrices generales que proporcionarán innovación, competitividad y crecimiento, y que, además, ayudarán a la difusión de las plataformas de las PYMES y de las empresas nacientes en

[22] https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:52020PC0842

todo el mercado único. Estas normas comunes poseerán un marco único y claro en toda la Unión Europea.

A continuación, vamos a analizar que sujetos estarían subyugados a la Ley de Mercados Digitales Esta ley solo será aplicable a las organizaciones nombradas como "guardianes de acceso" que, como he señalado anteriormente, son compañías con una gran relevancia y peso en del mercado interior debido a su gran tamaño y su importancia como nexo entre empresas y usuarios finales. Se debe cumplir una serie de condiciones para que una empresa sea denominada como guardián de acceso y pase a ser regulada por la Ley de Mercados Digitales:

- Que la empresa en cuestión alcance un volumen de negocios en el EEE[23] (Espacio Económico Europeo) por una cantidad igual o mayor a siete mil quinientos millones de euros cada año durante los tres últimos, o bien que su valor de mercado en el último año sea de setenta y cinco mil millones de euros y suministres algún servicio fundamental en todo caso a tres Estados miembros.
- Que la organización sea una importante mediadora entre usuarios y consumidores, es decir, que la empresa en cuestión explote un servicio que posea de media más de cuarenta y cinco millones de clientes mensuales ubicados en la Unión Europea y más de diez mil clientes profesionales anuales activos.
- Que la empresa cumpla los dos anteriores apartados durante los últimos tres años. Es lo que se conoce como una posición arraigada y duradera.

No obstante, la Comisión de la Unión Europea será la encargada de dar comienzo a diversas investigaciones para estimar específicamente la situación de una empresa u organización determinadas y tomar la decisión de si habría que definirla como "guardián de acceso". Aunque estas empresas contarán con la oportunidad de exponer argumentos para mostrar que no deberían ser nombradas como guardianes de acceso pese a que obedezcan estos requisitos. Las consecuencias de que una empresa sea definida como guardián de acceso son múltiples.

[23] El Espacio Económico Europeo (EEE) reúne a los Estados miembros de la UE y a tres de los cuatro Estados de la AELC (Islandia, Liechtenstein y Noruega) en un mercado interior regulado por las mismas normas básicas. La finalidad de estas normas es posibilitar la libre circulación de bienes, servicios, capitales y personas en todo el EEE en un entorno abierto y competitivo. El Acuerdo sobre el Espacio Económico Europeo entró en vigor el 1 de enero de 1994. https://www.eesc.europa.eu/es/tags/el-espacio-economico-europeo

En primer lugar, deben garantizar un ambiente accesible y justo para todas las organizaciones y consumidores a través del cumplimiento de las medidas instauradas en el proyecto legislativo. Por supuesto estas empresas estarán supeditadas a algunas obligaciones y prohibiciones. Deben lograr que los mercados sean más abiertos y discutibles, y por supuesto no acogerse nunca a prácticas ni comportamientos desleales. Si se da el caso de que en un futuro cercano alguna empresa pueda lograr gozar de una posición arraigada y duradera se le deberá atribuir una serie de obligaciones para evitar que no logre esa posición a través de prácticas desleales.

La ley de mercados digitales instaura una serie de obligaciones que estas empresas elegidas estarán obligadas a incluirlas en sus acciones del día a día para así asegurar un mercado digital justo y abierto. Estas medidas darán a las organizaciones la probabilidad de mejorar en cuanto a innovación y de disputarse mercados dependiendo de la superioridad de sus servicios y productos. Entre las obligaciones más importantes que tienen los guardianes de acceso se encuentra en las siguientes: dar la posibilidad a los usuarios de desinstalar con facilidad *apps* todavía no instaladas o modificar la configuración predeterminada de los sistemas operativos, los chatbots[24], o los buscadores web que los guían a los servicios y productos del guardián de acceso y dar a elegir entre diferentes pantallas para los servicios básicos.

Esta Ley también da opción a los clientes de cancelar sus suscripciones a las prestaciones más básicas encontradas en la plataforma de esta empresa denominada guardián de acceso con la misma sencillez con la que se suscribieron a ella, dar libertad de compartir datos y posibilitar el intercambio de información y conocimiento entre diferentes empresas con un fin próspero y positivo para los mercados digitales, dar permiso a los clientes profesionales para que den promoción a sus ofertas y realicen contratos con sus usuarios una vez fuera de la plataforma del guardián. Y por último facilitar a los clientes entrada o accesibilidad a la información que ellos mismos generen al utilizar esta plataforma propiedad del guardián de acceso.

Como hemos mencionado antes estas organizaciones denominadas guardianes de acceso poseen también una serie de prohibiciones entre las cuales se encuentran: la prohibición del uso de la información de los clientes cuando los guardianes de acceso sean

[24]Chatbot: es una aplicación de inteligencia artificial (IA) que puede imitar una conversación real conversación con un usuario con un lenguaje natural. Los chatbots permiten una conversación vía texto o por métodos auditivos en páginas web, aplicaciones de mensajería, aplicaciones móviles o por teléfono. https://sendpulse.com/latam/support/glossary/chatbot

rivales de estos, tienen prohibido organizar sus servicios de forma ventajosa respecto a los presentados por otros clientes, no podrán ordenar a los desarrolladores de *apps* que usen ciertos servicios propiedad de las plataformas guardianas para que figuren en sus tiendas de *apps* (algunos de estos servicios pueden ser sistemas de pago o bien proveedores de identidad[25]) y por último pero no menos importante estas empresas no podrán rastrear a los clientes una vez estos no se encuentren dentro del servicio principal de la plataforma con la finalidad de ofrecer publicidad personalizada sin el claro consentimiento del usuario.

La Comisión Europea, encargada de proponer legislación, hacer que se apliquen las decisiones comunitarias, proteger los tratados de la Unión Europea y ocupada de las cuestiones diarias de la Unión, será también la institución encargada de hacer cumplir, en este caso, los preceptos recogidos en la Ley de Mercados Digitales. Por lo tanto, de ocupará de preservar y mantener la armonización del mercado digital con la mayor de las seguridades jurídicas para todas las organizaciones de la Unión Europea.

Esta institución también será la encargada de coordinar rigurosamente con los mandos correspondientes y los tribunales el entorno de la supervisión de esta nueva Ley. El convenio pactado vaticina que, cuando esta institución esté prevista a tales efectos dentro del reglamento a nivel nacional, las competencias de cada país podrán poner en funcionamiento las normas de análisis para, de esa manera, establecer el incumplimiento por parte de la empresa protectora de la Ley de Mercados Digitales e informar del resultado a la Comisión Europea. Esto garantizará, en mayor medida, un alto nivel de cumplimento de las normas de esta Ley.

Según los artículos 101[26] y 102[27] del Tratado de Funcionamiento de la Unión Europea quedan prohibidos los acuerdos entre empresas y las prácticas abusivas que desemboquen en una alteración del correcto funcionamiento del comercio entre los Estados Miembros de la UE tales como: fijar directa o indirectamente los precios de compra o de venta u otras condiciones de transacción, limitar o controlar la producción, el mercado, el

[25] Proveedor de identidad (IdP): es un servicio que almacena y verifica la identidad del usuario. Los IdP suelen ser servicios alojados en la nube, y a menudo funcionan con proveedores de inicio de sesión único (SSO) para autenticar a los usuarios. https://www.cloudflare.com/es-es/learning/access-management/what-is-an-identity-provider/
[26] Artículo 101 TFUE: Serán incompatibles con el mercado interior y quedarán prohibidos todos los acuerdos entre empresas, las decisiones de asociaciones de empresas y las prácticas concertadas que puedan afectar al comercio entre los Estados miembros y que tengan por objeto o efecto impedir, restringir o falsear el juego de la competencia dentro del mercado interior.
[27] Artículo 102 TFUE: Será incompatible con el mercado interior y quedará prohibida, en la medida en que pueda afectar al comercio entre los Estados miembros, la explotación abusiva, por parte de una o más empresas, de una posición dominante en el mercado interior o en una parte sustancial del mismo.

desarrollo técnico o las inversiones o repartirse los mercados y las fuentes de abastecimiento (según el artículo 101) o imponer directa o indirectamente precios de compra, de venta u otras condiciones de transacción no equitativas, limitar la producción, el mercado o el desarrollo técnico en perjuicio de los consumidores y aplicar a terceros contratantes condiciones desiguales para prestaciones equivalentes, que ocasionen a éstos una desventaja competitiva (según el artículo 102).

Como toda ley, la de mercados digitales también posee una base jurídica, se trata del artículo 114 del TFUE en el cual se estipula que a no ser que los Tratados ordenen otra cosa, se procederá a aplicar las disposiciones necesarias para alcanzar los siguientes objetivos pertenecientes al artículo 26 del Tratado de Funcionamiento de la Unión Europea: 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; 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; 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.

Así pues, la Ley de Mercados Digitales será la responsable de que disminuya el nivel de prácticas desleales entre empresas y para con los usuarios, sin restringir la capacidad de la Unión Europea para posteriormente, interponerse a través de la adaptación de las medidas de competencia vigentes.

Estas normas serán aplicables una vez esté aprobada formalmente la Ley, la cual adoptará la forma jurídica de un Reglamento. Esta, entra en vigencia a los veinte días de su comunicación en el Diario Oficial de la Unión Europea[28] y su puesta en funcionamiento será a partir del sexto mes. Las empresas denominadas guardianes de acceso poseerán un período de seis meses para asegurar la ejecución de las normas implantadas en la Ley de Mercados Digitales a partir del nombramiento de la Comisión Europea como guardián de acceso. Esta designación comenzará a los seis meses de la entrada en vigor de esta Ley y en el momento que se pueda aplicar, cualquiera de las empresas que cumplan los requisitos vistos anteriormente podrá ser nombrada como tal. La Comisión Europea tendrá

[28] Diario Oficial de la Unión Europea: El Diario Oficial de la Unión Europea (DO) es la fuente principal de EUR-Lex. Se publica todos los días (de lunes a viernes; los sábados, domingos y festivos, solo en casos urgentes) en los idiomas oficiales de la UE. https://eur-lex.europa.eu/oj/direct-access.html?locale=es

un total de cuarenta y cinco días laborables para determinar si una empresa será nombrada guardián de acceso.

En definitiva, esta Ley de Mercados Digitales pretenderá terminar con el exceso y abuso de poder con el que cuentan muchas de las grandes empresas tecnológicas y posibilitar que otras pequeñas empresas puedan acceder al mercado y así ofrecer sus productos y servicios. En otro orden de ideas, esta ley podrá proporcionar a los clientes y consumidores mayores beneficios, aportándoles derechos y libertades dentro de plataformas privadas. Además de esto la institución encargada de proteger y hacer cumplir esta ley, la Comisión Europea, podrá imponer fuertes sanciones, entre ellas económicas de hasta el 10% del volumen de facturación total mundial en el periodo de un año, o bien una multa coercitiva del 5% del volumen de facturación medio diario a las organizaciones que incumplan su cometido. Esta Ley se revisará cada tres años.

5.2. Normativa sobre servicios digitales

5.2.1. Ley de Servicios Digitales

Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a un mercado único de servicios digitales (Ley de servicios digitales) y por el que se modifica la Directiva 2000/31/CE[29]. Los servicios digitales abarcan muchas categorías de servicios en línea, desde los sitios web más sencillos hasta las infraestructuras de centros de datos y plataformas online más elaborados y complejos. Las normas de esta ley se aplican s los mediadores y plataformas online como pueden ser las redes sociales, tiendas para apps, sitios web de viajes y alojamiento, mercados online y plataformas para compartir contenidos. Esta ley, junto a la anterior comentada, tiene el objetivo de consolidar los patrones para conseguir un internet más cierto y claro, además de esto también tiene como objetivo lograr que existan unas normas de competencia justas para las organizaciones de Unión Europea. Estas normas, que recaen directamente sobre las empresas intermediarias, descubrirán oportunidades nuevas con el fin de suministrar servicios electrónicos a través de las barreras, asegurando a la vez un altísimo nivel de seguridad para los clientes, independientemente de donde se sitúen dentro de la Unión Europea.

[29] https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:52020PC0825

Como ya mencioné en el inicio de este trabajo, durante estos últimos años han surgido diversas e innovadoras formas de comunicarse, comprar o acceder a información on-line y siguen en continua evolución. La Unión Europea debe asegurarse de que la legislación europea crezca y progrese con estos cambios. Las plataformas virtuales han supuesto importantes beneficios para clientes, consumidores e innovación, y han contribuido a la mejora para conseguir ser más eficiente del mercado interior de la Unión Europea. Además de esto han promovido el comercio a través de las fronteras interiores y exteriores de la UE. Esto ha supuesto nuevas coyunturas para una diversidad de organizaciones y comerciantes europeos al favorecer su ampliación y entrada a nuevos mercados.

Es cierto que existe un acuerdo adoptado entre todos los países miembros de la Unión Europea el que se debaten los grandes beneficios que esta transformación digital trae consigo, pero al igual que aporta cosas buenas, también surgen ciertos problemas que tienen una repercusión negativa tanto para la sociedad como para la economía. Una de las principales preocupaciones que genera esta transformación es el intercambio de bienes, servicios y contenidos ilegales on-line. Estos servicios son unas herramientas mal utilizadas con el objetivo de manipular, a través de algoritmos, para incrementar la divulgación de la desinformación con la intención de resultar perjudiciales. Estos retos innovadores y la manera en las que las empresas y plataformas en línea los plantean tiene un efecto muy relevante en los principales derechos on-line.

A causa de todo este proceso de digitalización tan veloz, se ha conseguido que unas pocas plataformas digitales de gran tamaño dominen comunidades de gran importancia en la economía digital, con el poder de ejercer como legisladores privados. Esto ha provocado situaciones injustas en cuanto a las condiciones que se les proporcionan a las empresas y consumidores que usan estas plataformas. Con el desarrollo de este marco legal en el que el amparo de los derechos fundamentales es clave, así como la protección de los clientes on-line y mantener un ambiente de seguridad, justo y abierto se pretende hacer de Europa una pionera en la seguridad digital.

Las normas establecidas en la Ley de servicios digitales promueven los avances, la competitividad entre empresas, la innovación y la oportunidad de crecimiento para las pequeñas y medianas empresas e incluso para las emergentes. Estas normas tienen la responsabilidad de defender y ayudar a los clientes y consumidores, así como sus derechos fundamentales entre ellos destacan: derecho a una información correcta, derecho a la

protección de los intereses económicos y sociales, derecho a la reparación de daños y perjuicios sufridos, derecho a la salud y a la seguridad…. Crear un ambiente basado en la transparencia, la claridad y la rendición de cuentas para las plataformas virtuales. Y por supuesto el de incitar a la innovación, el desarrollo y la rivalidad en el mercado único. Haciendo más sencillo y seguro a ciudadanos, proveedores de servicios digitales y empresas usuarias de estos servicios el uso de las nuevas tecnologías.

Los negociadores del Parlamento Europeo y de la Comisión Europea han llegado a un acuerdo político sobre esta reciente ley de servicios digitales a través de la cual van a tomar medidas contra las informaciones ilegales que se encuentran en Internet y poner freno a la desinformación online. Esta Ley se aplicará a todos los mediadores online que suministren servicios dentro de la Unión Europea y perjudicade alguna manera a los gigantes tecnológicos que, una vez entre en vigor, deberán llevar a cabo un análisis anual para reducir los peligros vinculados a la divulgación de contenidos ilegales o la manipulación de servicios. La ley, además, incluye un concepto bastante innovador, conocido como responsabilidad algorítmica a través del cual la Comisión Europea, así como los estados miembros, poseerán acceso a los algoritmos de las grandes compañías tecnológicas, las cuales estarán forzadas, una vez se cumpla el establecimiento e implantación de esta ley, a suprimir los productos, servicios o contenidos ilegales en el instante después de que estos hayan sido denunciados.

La ley también pone frontera a los patrones oscuros de la web, esto se refiere a triquiñuelas usadas por algunas aplicaciones o sitios web con el objetivo de influir, generalmente de forma negativa en la conducta de la gente, además, están destinados a la explotación económica de sus clientes por medio de preguntas engañosas, escasez o carencia de comparaciones de precios o bien de la creación de barreras artificiales para dar de baja ciertos servicios.

Esta nueva legislación también obliga a que cualquiera de las plataformas a la que puedan acceder menores de edad implanten medidas adecuadas de protección con el fin de garantizar su seguridad si se produjera el incumplimiento de este acuerdo. Las plataformas online y los motores de búsqueda podrían recibir unas sanciones de hasta el 6 % de su facturación a nivel mundial[30]. La institución de la Comisión Europea será la que posea el poder exclusivo para reclamar dicho cumplimiento.

[30] https://www.reasonwhy.es/actualidad/acuerdo-europeo-ley-servicios-digitales-internet-seguro-responsable

5.2.2. El nuevo Reglamento sobre Servicios Digitales

El pasado 19 de octubre del presente año ha entrado en vigor una nueva ley que modifica la norma anteriormente citada. Será de aplicación dentro de 15 meses, es decir, aproximadamente a principios del año 2024, las principales modificaciones que se han introducido son las siguientes:

- Las Pymes y microempresas (empresas de menos de 50 trabajadores y facturación total anual no superior a 10 millones de euros) quedan totalmente eliminadas de las obligaciones especiales de las plataformas on-line.
- La creación de una nueva figura conocida como *"alertadores fiables".* Estas figuras principalmente son entidades, las cuales hayan garantizado poseer conocimientos y capacidades específicos para revelar, reconocer y notificar contenidos ilícitos y que no posean un vínculo con los prestadores de servicios.
- La exigencia de que los grandes prestadores de servicios creen sistemas de gestión de reclamaciones, solicitudes o demandas que asegure que las decisiones específicas sobre contenidos ilícitos puedan ser refutadas por los clientes gratuitamente.
- Y por último la claridad de los anuncios ofrecidos on-line, requiriendo que las plataformas den información sobre aquel contenido que, efectivamente, es publicitario, la organización, servicio o producto al que se esté dando promoción y las medidas utilizadas para establecer la audiencia del anuncio, como por ejemplo la lógica aplicada. Es también importante la novedad dentro de esta reforma de la ley que da permiso a las plataformas online para suspender de forma temporal a los creadores que posean un comportamiento inmoderado en su entorno, como anunciar con frecuencia contenido ilegal o impedir el correcto funcionamiento de las propias plataformas.

5.3. Ley de Inteligencia Artificial

Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de Inteligencia Artificial (LEY DE INTELIGENCIA ARTIFICIAL) y se modifican determinados actos legislativos de la Unión[31]. A lo largo de los años la Comisión Europea ha estado promoviendo la colaboración en

[31] https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex:52021PC0206

inteligencia artificial a lo largo de toda la Unión europea para estimular y promocionar la rivalidad y asegurar la franqueza fundamentada en los principios de la Unión Europea. En 2018 se publicó la Estrategia Europea sobre IA y en 2019 se desarrollaron las Directrices para una inteligencia artificial fiable y una carpeta de evaluación para 2020 que acabaron desembocando en lo que actualmente conocemos como Ley o Reglamento de Inteligencia Artificial.

La correcta utilización de la Inteligencia Artificial dentro de las empresas y en nuestra vida cotidiana puede suponer una mejora de calidad y de eficacia en todos los ámbitos que nos rodean en el día a día, nos podría ayudar a dar con las claves de muchas de las controversias de la sociedad. Esto puede sólo conseguirse si esta Inteligencia llega a conseguir la seguridad y confianza de la población. Así que, una ley basada en las virtudes de la Unión Europea puede proporcionar a los ciudadanos y las empresas la valentía necesaria para apoyarse en la Inteligencia Artificial. Este Reglamento asegurará tanto una tecnología fiable como la seguridad y la protección de los usuarios y las organizaciones que la utilicen.

Esta Ley, que tiene como objetivo mejorar y proporcionar más estabilidad, ética y justicia en la Unión Europea en el ámbito de la digitalización de las empresas. Otro de los objetivos que se encuentra dentro de los principales es el de favorecer el avance y el crecimiento tanto como la aceptación de la Inteligencia Artificial. Para que esto tenga éxito, será necesario la elaboración de un plan coordinado entre los países miembros de la UE y la Comisión Europea con unas estrategias enfocadas a activar y poner en marcha las inversiones en la Inteligencia Artificial y sus tecnologías para así estimular una restauración tanto económica como comunitaria con el apoyo de los actuales remedios digitales. Esto se conseguirá haciendo de la Unión Europea un lugar donde la IA actúe siendo un apoyo para las personas y sirva para la edificación de un liderazgo en el ámbito del uso de las nuevas tecnologías.

Ley, que se propuso para su regulación por la Comisión Europea el 21 de abril del 2021 con el objetivo de establecer reglas para la inclusión, el comienzo y el uso de sistemas de inteligencia artificial (IA)[32] en toda la Unión Europea, así como vetos de ciertas prácticas

[32] Sistema de inteligencia artificial (sistema de IA): el software que se desarrolla empleando una o varias de las técnicas y estrategias que figuran en el anexo I y que puede, para un conjunto determinado de objetivos definidos por seres humanos, generar información de salida como contenidos, predicciones, recomendaciones o decisiones que influyan en los entornos con los que interactúa. https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex:52021PC0206

de inteligencia artificial. Los operadores y los sistemas de inteligencia artificial de alto riego deberán de cumplir una serie de requisitos, pero ante todo esta ley establece normas de control sobre el mercado.

La Ley de Inteligencia Artificial se aplicará sobre los suministradores que importen sistemas de IA a la Unión Europea independientemente de si estos proveedores están, o no, dentro de la UE o en un país tercero. También se aplicará sobre los clientes y usuarios que se encuentran dentro de la UE, incluidos también los clientes y suministradores que se encuentren en países terceros y la información de salida generada por ese sistema en concreto se acabe utilizando en la UE. Este reglamento no será aplicable a los sistemas de IA que han sido fabricados o van a ser utilizados con objetivos únicamente militares. Tampoco se aplicará a los mandatarios públicos de países terceros ni tampoco a las sociedades internacionales que se introduzcan en el sector de la aplicación de este Reglamento siempre y cuando estas autoridades y organizaciones usen los sistemas de Inteligencia Artificial dentro del ámbito de convenios internacionales teniendo como meta la aplicación de la norma y colaboración judicial con la UE o con alguno de los Estados Miembros.

Las normas que propone este Reglamento plantearán los diferentes riesgos que pueden sugerir estos sistemas de IA y determinarán diferentes estándares de riesgo, a saber (de más peligrosidad a menos): riesgo inaceptable, alto, limitado y mínimo. Estas normas se emplearán en toda la Unión Europea y sus países miembros. Procedamos a analizar las diferentes clases de riesgos existentes:

- Riesgo inaceptable: quedarán totalmente prohibidos los sistemas considerados como un claro peligro para la fiabilidad, derechos y protección de los usuarios. Incluidos los que manipulen la conducta de las personas con el fin de inculcar un libre comportamiento entre los usuarios.
- Riesgo alto: se identifican como riesgo alto los sistemas de Inteligencia Artificial que son utilizados en infraestructuras que cabe la posibilidad de que pongan en peligro la vida de la población.
- Riesgo limitado: sistemas con el deber de poseer claridad y transparencia, como es el caso de los chatbots, de los que hablé anteriormente, en este caso, el cliente debe saber que se está interrelacionando con una maquina y a partir de ese momento, tener la determinación para seguir adelante o retroceder.

- Riesgo mínimo: la inmensa mayoría de sistemas de IA componen esta categoría de riesgo mínimo. Este Reglamento del que hablamos no toma parte en esta categoría ya que el peligro que suponen estos sistemas es apenas existente para los derechos o la protección de la población.

La Comisión Europea se responsabilizará para promover e impulsar los avances en el crecimiento y utilización de las tecnologías de inteligencia artificial en todas las organizaciones de los Estados Miembros. La organización hará la situación de liderato de la Unión Europea en Inteligencia Artificial basada en el ser humano, duradera, fehaciente, incluyente y fiel. Este Reglamento tuvo su principio en 2018 cuando se publicó por primera vez un Plan Coordinado sobre IA, el cual hizo posible obtener una vista excitante y prometedora sobre los planes de redes de investigación e innovación para organizaciones públicas y privadas de la UE.

La versión más actualizada de este Plan Coordinado plantea actuaciones grupales en determinados momentos de colaboración para así asegurar que todas las dificultades estén ordenados con la Estrategia Europea sobre Inteligencia Artificial y el Pacto Verde Europeo[33] sin obviar las nuevas dificultades que propone la pandemia del Coronavirus. Muestra un punto de vista para precipitar las inversiones en inteligencia artificial lo que puede ayudar a su mejoría. Otro de los objetivos es el de incentivar la puesta en funcionamiento de estrategias estatales de IA, terminar con la fragmentación e iniciar los problemas globales.

El Plan Coordinado sobre IA actual usará el capital designado por los programas Europa Digital, el cual fue antes mencionado, y Horizonte Europa[34]. Gracias a esto se crearán situaciones favorables para el avance y la afiliación de la inteligencia artificial por medio del intercambio de información y de datos, se asegurará que la IA trabaje para los seres humanos y sirva de punto de apoyo para hacer el bien en la sociedad, así como que promoverá talentos y nuevas habilidades. También construirá un liderato en ámbitos como el del medioambiente, la movilidad, la sostenibilidad, el sector agroalimentario y la robótica.

[33] Pacto Verde Europeo: El Pacto Verde Europeo es un paquete de iniciativas políticas cuyo objetivo es situar a la UE en el camino hacia una transición ecológica, con el objetivo último de alcanzar la neutralidad climática de aquí a 2050. Es la base para la transformación de la UE en una sociedad equitativa y próspera con una economía moderna y competitiva. https://www.consilium.europa.eu/es/policies/green-deal/#:~:text=%C2%BFQu%C3%A9%20es%20el%20Pacto%20Verde,clim%C3%A1tica%20de%20aqu%C3%AD%20a%202050.

[34] Horizonte Europa: Horizonte Europa es el programa marco de investigación e innovación (I+I) de la Unión Europea (UE) para el período 2021 -2027. El Programa Horizonte Europa, como su predecesor Horizonte 2020, será el instrumento fundamental para llevar a cabo las políticas de I+D+I de la UE.

El futuro de este Reglamento descansa en la aprobación del Parlamento Europeo y los Estados Miembros de las medidas que serían adoptadas y directamente aplicables con futuras medidas comunicadas en el Plan Coordinado.

A todo lo anterior hay que añadirle que esta será la primera legislación sobre Inteligencia Artificial del mundo. No ha sido rápido ni sencillo ya que se han necesitado un total de 18 meses para que los diputados europeos de los distintos grupos políticos estuvieran de acuerdo. Otra de las finalidades con las que cuenta esta legislación es la de ser una legislación semejante a la del Reglamento General de Protección de datos, del que hablaremos a continuación. Se espera que, a finales del presente año, 2022, se realice una proposición completa para que en el posterior año se apruebe y la Unión Europea cuente con la primera legislación de IA en el mundo.

5.4. Real Decreto-Ley de servicios de pago y otras medidas urgentes en materia financiera

El 25 de noviembre de 2018 entró en vigor el Real Decreto-Ley 19/2018, de 23 de noviembre, de servicios de pago y otras medidas urgentes en materia financiera. La importancia de este Real Decreto está, fundamentalmente, en la trasposición de la Directiva de la Unión Europea 2015/2366, del Parlamento Europeo y del Consejo, de 25 de noviembre de 2015, sobre servicios de pago en el mercado interior, también conocida como PSD2.

La finalidad de este real decreto-ley es la regulación de los servicios de pago que se consideren de carácter profesional en nuestro territorio, además de la forma de prestación de los servicios, el régimen jurídico de aquellas que realicen servicios de pago, el régimen de transparencia e información que se aplica a las entidades y por último los derechos y obligaciones de los usuarios de estos servicios y de los proveedores de los estos.

La existencia de un buen mercado de servicios de pago supone un requisito básico en la instauración de un mercado único efectivo dentro de la Unión Europea. Con este objetivo, la regulación de los servicios de pago debe promover especialmente un ambiente que favorezca el desarrollo ágil de las transacciones de pago, unas normas que sean comunes en lo que atañe a su operatividad, y unas pautas de auxilio efectivas a los clientes de servicios de pago. La seguridad y la similitud en los métodos de pago son clave en el

aumento de la eficiencia y la disminución de los costes de dichos métodos, tanto a nivel nacional como en los pagos realizados entre los Estados miembros.

Que los usuarios exijan un sistema de autenticación reforzada en cuanto a la identificación implica una garantía adicional de seguridad para ellos a la hora de prevenir las malas consecuencias de, por ejemplo, una compra o de un acceso a una página web fraudulenta. En caso de que se realicen operaciones no autorizadas, el usuario no será deberá correr con el gasto.

Estos sistemas de autenticación reforzada, consisten esencialmente en que para dar por válida una operación deben combinarse la utilización de dos o más elementos. Estos instrumentos que se utilizarán para proteger la seguridad de la transacción deben ser:

- Algo que únicamente el cliente conozca, por ejemplo, una contraseña.
- Algo que únicamente el usuario posea, por ejemplo, un móvil donde reciba un SMS para confirmar la operación.
- O bien algo propio del cliente como puede ser la huella digital.

Además de esto, los instrumentos mencionados deben ser independientes entre sí, de forma que, si un ciberdelincuente consigue hackear la contraseña, no tenga modo alguno de conseguir los otros instrumentos. Debido a esto, se han establecido una serie de exigencias que deben desempeñar todos los métodos.

- Por lo menos uno de los instrumentos no debe haber sido robado a través de Internet (la huella dactilar).
- Por lo menos uno de estos elementos no debe ser reutilizable, esto significa que la contraseña por autentificación generada sea única y no pueda usarse en otra operación diferente.
- Por lo tanto, esta normativa proporciona libertad a todas las entidades para que determinen los mecanismos que va a utilizar en cada caso.

6. Problemas claves a resolver

6.1. La Ciberseguridad

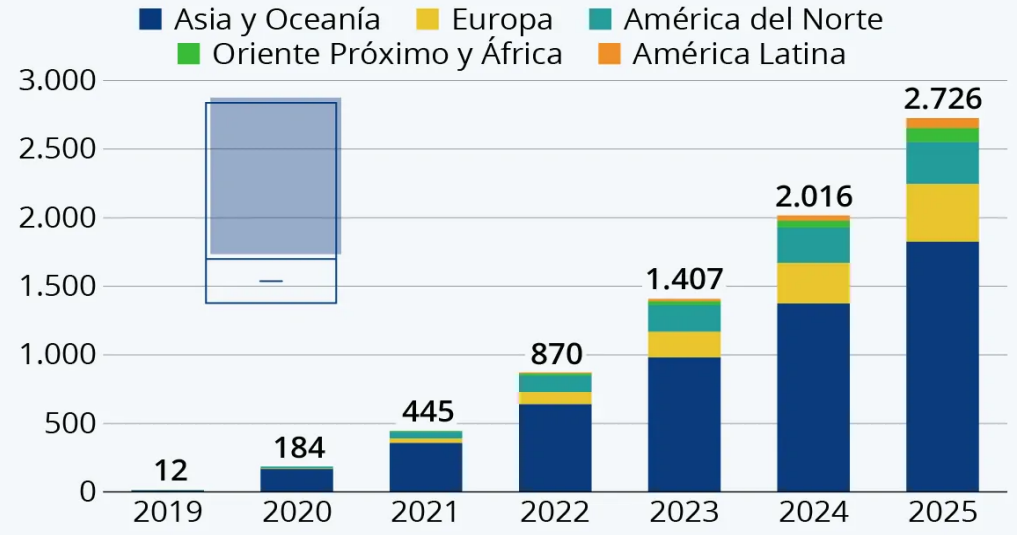
La ciberseguridad es la habilidad de defender sistemas, redes y programas de ataques digitales. En relación al informe del Panorama actual de la Ciberseguridad en España preparado por The Cocktail Analysis[35]. La Europol, establece que "los ciberataques son cualquier delito que solo se puede cometer utilizando ordenadores, redes informáticas y otras formas de tecnología de comunicación de la información (TIC)" (p.23). Normalmente, estos ciberataques se orientan a acceder, modificar o destruir la información privada y confidencial de empresas, gobiernos y, en general, de cualquier tipo de usuario, a los que además se extorsiona. El crecimiento global de las redes y la información, impulsado por la innovación tecnológica, ha permitido a la sociedad crear prosperidad y mejorar la calidad de vida. Sin embargo, este rápido cambio ha generado también un desafío de largo plazo: gestionar los riesgos de seguridad a medida que el mundo depende cada vez más de la cibernética y las amenazas aumentan.

Es un hecho que, en los siguientes años, el nivel de inserción de la digitalización no parará de crecer en todos los aspectos de la vida humana, la gestión empresarial y de recursos públicos a nivel mundial. Por lo que, también se acrecentarán sus riesgos.

El número de ciberataques crecerá. Al igual que también aumentará su dificultad y la repercusión de aquellos que tengan éxito. Por ello, la ciberseguridad pasará a ser una completa prioridad para lograr mantener un funcionamiento apropiado del mercado, de la convivencia social y del sistema de derechos y libertades.

[35] https://www.ospi.es/export/sites/ospi/documents/documentos/Seguridad-y-privacidad/Google_Panorama-actual-de-la-ciberseguridad-en-Espana.pdf

Gráfico 4 Número estimado de suscripciones móviles a redes 5G por región (en mill.)



Fuente: Statista[36]

Esta gráfica está realizada con los datos de una previsión realizada en el año 2020 por la empresa sueca Ericsson. La aparición del 5G y la propensión a pasar todo a la nube significarán el punto de inflexión. Según esta empresa, si en el año 2019 había 12 millones de dispositivos conectados a redes 5G, en el año 2025 habrá 2 736 millones. Debido a esto, si no nos garantizamos de aportar al sistema suficiente seguridad, un solo ataque cibernético podrá afectar a toda la red en seguida.

Exactamente lo mismo ocurrirá con el Internet de las Cosas (IoT) y la inteligencia artificial (IA). La conectividad entre dispositivos va a mejorar en un primer momento: la vida personal y pública de los individuos y la gestión de las organizaciones, sin embargo, también va a abrir paso a nuevos métodos de ciberdelincuencia.

6.1.1. Ciberseguridad en Europa

Debido a que las instituciones, órganos y organismos de la UE (IOUE) manejan una información de una relevancia muy importante, son claros objetivos para los potenciales atacantes, en concreto para los grupos capaces de elaborar ataques sigilosos con propósitos de ciberespionaje y otros fines. Los ciberataques contra estas instituciones y

[36] https://es.statista.com/grafico/16309/numero-de-suscripciones-moviles-a-redes-5g/

organismos de la UE que llegan a completarse pueden tener importantes alcances políticos, perjudicar la reputación general de la UE y quebrantar la confianza en sus instituciones.

La pandemia de COVID-19 ha forzado a las IOUE, así como a otras instituciones de todo el mundo, a acelerar bruscamente la transformación digital y a asumir el trabajo a distancia como uno más. Esto ha hecho que aumente de manera considerable el número de posibles puntos de entrada para los asaltantes (a esto se le denomina "superficie de ataque"), al aumentar el ámbito de actuación de las empresas a viviendas y móviles conectados a Internet, donde pueden aprovecharse nuevas debilidades. Los servicios de acceso remoto son una de las rutas más comunes a través de las cuales, los grupos que acometen amenazas contra las IOUE, consiguen acceso inicial a sus sistemas.

La cantidad de ciberincidentes[37] va en aumento y una corriente especialmente alarmante es el increíble aumento de hechos significativos que dañan las IOUE; en el anterior año se ha batido el récord de ataques a estas instituciones y organismos. Normalmente, estos ataques suponen la utilización de métodos y tecnologías innovadores y pueden durar semanas o incluso meses de investigación y de recuperación. Estos incidentes se multiplicaron por diez entre 2018 y 2017. Por lo menos veintidós IOUE han sido víctimas de incidentes significativos. Un caso reciente fue el ciberataque dirigido a la Agencia Europea de Medicamentos, que tuvo como consecuencia la filtración y manipulación de información delicada con el objetivo de hacer disminuir la confianza en las vacunas.

Actualmente Internet supone un factor clave en la vida de cualquier europeo. Su desarrollo exponencial, así como el aumento constante de usuarios en las redes han puesto una cuestión sobre la mesa que conforme va pasando el tiempo preocupa más a los ciudadanos, la seguridad.

Las infracciones de seguridad, las cuales se han reiterado en el tiempo, han causado tanto daños económicos a los usuarios, como una interrupción del desarrollo del *e-commerce*. Pero no solo preocupan estos asaltos, los sistemas informáticos y las redes de comunicación también son bastantes delicados. Un fallo en estas redes y el suministro de cuantiosos servicios, algunos de ellos indispensables para el bienestar de los ciudadanos de la Unión Europea, se vería comprometido.

[37] Ciberincidente: cualquier acontecimiento que pueda significar un peligro para la seguridad de las redes y sistemas de información de una empresa o un particular, ya sea ocasionado por un individuo intencionadamente o a causa de una mala práctica.

Cómo remedio para combatir contra las actividades ilegales en internet la UE ha creado una innovadora política de ciberseguridad, que está fundamentado en la importancia del amparo tanto de los individuos como de las redes de comunicación y los sistemas informáticos y de información frente a los posibles ataques.

Esta política se aprecia en acciones como la creación del sistema "Safer Internet Plus" ejecutado durante 2005-2008 cuyo objetivo era el de buscar un internet más sólido que protegiera al usuario frente a contenidos no deseados. Este sistema fue perfeccionado por otro siguiente llamado "Safer Internet" durante los años 2009-2013 cuya propuesta era la de mejorar la seguridad online de los más pequeños luchando contra los contenidos ilícitos y los comportamientos nocivos.

Además de estos dos programas, se han desarrollado una serie de operaciones como la fundación de la Agencia Europea de Seguridad de las redes y de la información (ENISA), destinada a lograr un nivel muy elevado de ciberseguridad en la Unión Europea. El cometido de la ENISA, fundada en el año 2004, es aumentar la credibilidad de los productos, procesos y servicios de las tecnologías de la información y las comunicaciones (TIC) a través de sistemas de certificación de la ciberseguridad, colaborar con las IOUE y los Estados miembros, y ayudarles para prevenir las ciberamenazas. La ENISA auxilia a las IOUE en el perfeccionamiento de capacidades y en colaboración operativa.

Uno de los principales objetivos de la Agencia es el de renovar las facultades de la Unión Europea, sus Estados Miembros y las organizaciones e instituciones en relación a la previsión, la reacción y la gestión de los inconvenientes pertenecientes a la seguridad de las redes y la información. No es este el único objetivo, ya que también ofrece soporte y asesoramiento a la Comisión Europea y a los Estados miembros cuando se le requiere.

La Agencia lleva a cabo una serie de funciones para cumplir con los objetivos anteriormente mencionados. Entre estas funciones se encuentran la de recopilar información imprescindible para la investigación de los peligros actuales y emergentes, y facilitar los resultados obtenidos a la Comisión y a los Estados Miembros. La Agencia Europea de Seguridad de las redes y de la información es la encomendada para promover evaluaciones de riesgos y métodos de gestión de los mismos con el objetivo de mejorar la competitividad de la Unión Europea para hacer frente a los peligros de seguridad. También puede exponer sus propias conclusiones, orientaciones y sugerencias.

6.1.2. Ciberseguridad en España

En el año 2013 se creó la primera Estrategia Nacional de Ciberseguridad en España. El escrito establecía las directrices e indicaciones generales de actuación para hacer frente al desafío que supone la debilidad del ciberespacio. Igualmente, a lo largo de estos últimos 9 años, nuestro país ha seguido progresando en sus empeños por ayudar al desarrollo de un ciberespacio seguro y fiable. Uno de sus principales apoyos es el Consejo Nacional de Ciberseguridad, creado en el año 2014, medio de apoyo del Consejo de Seguridad Nacional.

Desde el primer día, el Consejo Nacional de Ciberseguridad ha aceptado la labor de coordinar los organismos con aptitudes en el ámbito a nivel nacional y la mejora del Plan Nacional de Ciberseguridad y sus planes derivados. Por lo que, a día de hoy, España tiene instituciones especializadas en ciberseguridad y una condición aventajada a nivel europeo e internacional. Del mismo modo, el marco jurídico ha experimentado también una importante adaptación. Como consecuencia de su evolución y la experiencia reunida en estos años, en 2015 se anunció la reforma del Esquema Nacional de Seguridad para asegurar la protección de los sistemas del Sector Público. Por otra parte, la entrada en vigencia del Real Decreto ley 12/2018 de 7 de septiembre[38], ha supuesto un logro importante en el perfeccionamiento de la ciberseguridad en España, prolongando la transcendencia de esta Directiva con la finalidad de mejorar la seguridad de la información de todos los sectores estratégicos.

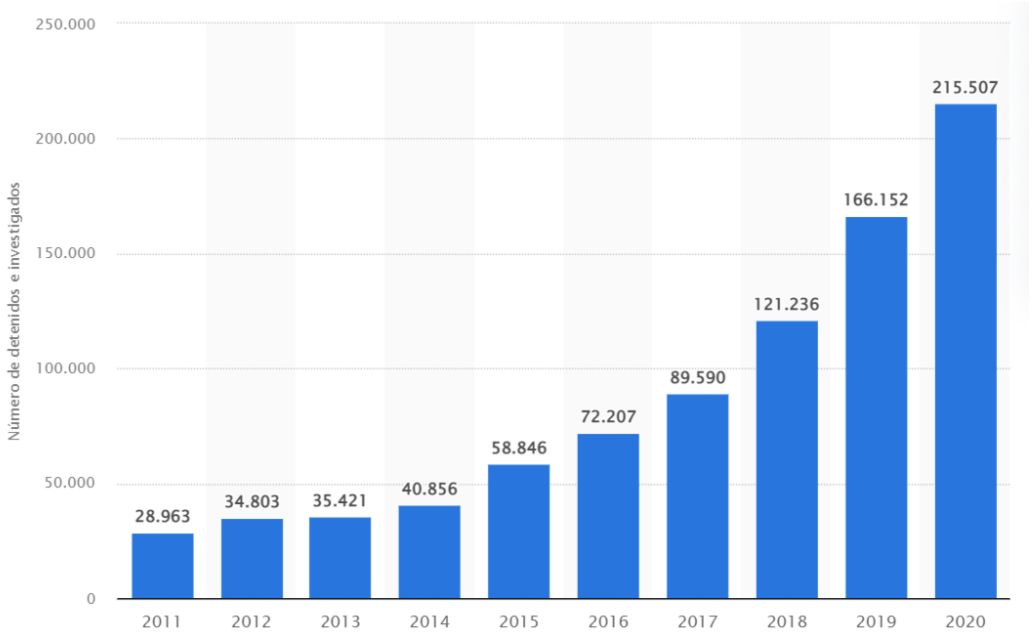
La Ley de Seguridad Nacional percibe la ciberseguridad como terreno de gran interés. Se puede decir que la ciberseguridad ha innovado la Seguridad Nacional, siendo uno de los ámbitos que más ha crecido hasta la fecha. La Estrategia de Seguridad Nacional de 2017 establece un punto de inflexión en la reflexión estratégica nacional, en el cual la ciberseguridad ha de situarse en un espacio propio y diferencial.

La Estrategia Nacional de Ciberseguridad 2019[39] sitúa la posición de España ante una reciente concepción de la ciberseguridad en el marco de la Política de Seguridad Nacional. Las líneas de acción de esta estrategia nacional constan de los siguientes objetivos:

[38] Artículo 1, apartado primero del Real Decreto-ley de seguridad de las redes y sistemas de información: Este Real Decreto tiene por objeto regular la seguridad de las redes y sistemas de información utilizados para la provisión de los servicios esenciales y de los servicios digitales, y establecer un sistema de notificación de incidentes.
[39] https://www.dsn.gob.es/es/documento/estrategia-nacional-ciberseguridad-2019

- Fortalecer las capacidades ante las amenazas procedentes del ciberespacio y asegurar la seguridad y resiliencia de los activos estratégicos para nuestro país.
- Fortalecer las capacidades de investigación y rastreo de la cibercriminalidad, para asegurar la seguridad ciudadana y la salvaguarda de los derechos y libertades en el ciberespacio.
- Promover la ciberseguridad de ciudadanos y empresas. Además de fomentar la industria española de ciberseguridad, y la generación y conservación de talento, para el fortalecimiento de la autonomía digital.
- Difundir una cultura de ciberseguridad y colaborar con la seguridad del ciberespacio en el ámbito internacional, impulsando un ciberespacio abierto, plural, seguro y confiable, en apoyo de los intereses nacionales.

Gráfico 5: Número de victimizaciones por ciberdelitos en España de 2011 a 2020



Fuente: Statista[40]

Este gráfico está elaborado a partir de los datos proporcionados por el Ministerio del Interior de España publicados en el año 2021. Lo que podemos observar en él es que las víctimas de cibercrímenes no han dejado de aumentar en nuestro país desde 2011. De este

[40] https://es.statista.com/estadisticas/814010/cibercrimen-numero-de-victimizaciones-espana/#:~:text=Las%20victimizaciones%20por%20cibercr%C3%ADmenes%20no,de%20los%20215.500%20en%202020.

modo, la totalización de víctimas que han sufrido estos delitos llegó a ser más de 215.500 en 2020.

El delito informático, también conocido como ciberdelito o cibercrimen, es el termino empleado para hablar de toda acción ilícita ejecutada principalmente a través de Internet usando materiales tecnológicos como ordenadores y *smartphones*, así como otros dispositivos portátiles. En el año 2020 en España tuvieron lugar más de 16 900 procedimientos judiciales por ciberdelincuencia según datos proporcionados por la fiscalía general del Estado[41]. Esto significa un aumento del 28,69% respecto al año 2019. De todos estos delitos la gran mayoría correspondí a ataques contra el patrimonio o la libertad.

El programa de ayudas para favorecer la digitalización en PYMES denominado Kit Digital, el cual hemos mencionado antes, servirá, para dar impulso al sector de la ciberseguridad en España. El director general del Instituto Nacional de Ciberseguridad[42] (INCIBE) Félix Barrio, establece que un 9% de los bonos proporcionados por este programa están empleándose a proyectos de compra y adquisición de servicios y resultados en ciberseguridad. La primera de las convocatorias ha ofrecido bonos de hasta 12 000 euros para pymes de entre 10 y 49 trabajadores, ya se han ofrecido unas 70 000 solicitudes y se han adjudicado unas 35 000. La segunda de las convocatorias, la cual comenzó hace unas semanas, está pensada para empresas de entre 3 y 9 trabajadores con unos bonos de 6 000 euros.[43]

Lo que quiere decir que, de mantenerse así el porcentaje, de los 3.100 millones de euros que tiene el Kit Digital, la cantidad destinada al campo de la ciberseguridad sobrepasaría los 300 millones de euros. Promover esa demanda nacional y ese mercado local de la ciberseguridad es de vital importancia por dos razones básicas: por la superioridad tecnológica y porque de esta manera se favorece a que las pymes, también tecnológicas, que han sido fuertemente azotadas durante la pandemia, puedan comenzar con su recuperación.

[41] https://es.statista.com/temas/3166/ciberdelitos-en-espana/#topicHeader__wrapper
[42] https://www.incibe.es/
[43] https://www.leonoticias.com/leon/jornadas-sobre-ciberseguridad-20221004105856-ga.html

6.1.3. Clases de ciberataques

Los timos y estafas llevan existiendo toda la vida, pero con los años han ido evolucionando, cuando hace un tiempo se usaban engaños simples por la calle, ahora se utilizan técnicas muy sofisticadas para conseguir información por medio de Internet. Tanto si eres una empresa como un usuario hay que ser muy precavido a la hora de introducir nuestros datos en los portales web ya que pueden ser fácilmente extraídos y puede significar la continuidad de la organización en caso de ser una empresa o la ruina total si eres un usuario.

Los ciberataques que un negocio o cualquier individuo pueden sufrir más fácilmente son los que atentan contra los datos e información. Dentro de la gran variedad de ataques cibernéticos existentes, hay dos que son, sin duda alguna, los más famosos y perjudiciales.

En primer lugar, hablaremos del ataque conocido como *"Phising"*. El fraude a través de esta técnica es bastante frecuente hoy en día. Por medio de esta técnica, se reproduce una página web de forma exacta, para que el individuo se piense que está metiendo sus datos en la misma, cuando en efecto, los está introduciendo en una página pirata, donde sus datos van a parar al ciberdelincuente

Para que se entienda mejor, voy a poner un ejemplo. De lo casos más habituales consisten en que se copie una página web de un banco y a continuación se mande el enlace de esta página a la víctima por medio de un correo electrónico, utilizando el pretexto de que debe cambiar su contraseña o que debe revisar un pago que se está cargando.

Este usuario afectado entra al enlace sin pensarlo debido al miedo, introduce sus datos, los cuales van a parar a la persona que está cometiendo el fraude y se produce un delito de estafa. Una vez está en posesión de los datos, el ciberdelincuente los cambia rápidamente y consigue el acceso a sus cuentas.

El segundo de los ciberataques del que vamos a hablar es el "*Ransomware"* o también conocido como malware de rescate el cual impide al usuario afectado acceder a sus datos y archivos personales. Se exige el pago a modo de rescate para poder recuperar y volver acceder a los archivos secuestrados.

Existen tres tipos de ransomware: el Scareware (en el cual intentan convencerte de que tus archivos están en peligro y si no pagas los perderás, siendo esto falso ya que a tus archivos no les pasa nada), Bloqueadores de pantalla (el cual impide el uso de tu ordenador

completamente apareciendo en la pantalla de tu PC un logo similar al del departamento de Justicia de EE.UU. o del FBI indicando que se han descubierto actividades ilícitas en su ordenador y ordenando pagar una multa. Esto es falso ya que de ser así las instituciones pertinentes actuarían bajo la legalidad y no ordenando el pago de una multa) y, por último, el más dañino y peligroso de todos es el llamado *Ransomware de cifrado* en el que se secuestra una serie de archivos y se cifran exigiendo como en todos, un pago por la descifrado y la devolución. La diferencia es que, en este caso, no existe garantía de la devolución de los datos por parte de los atacantes, aunque se realice el pago.

6.2. Protección de datos de carácter personal en el entorno digital

La regulación de la protección de datos está formada por una continuación de normas que específicamente regularizan todos o la mayoría de marcos en el tratamiento de ciertos tipos de información. Estas reglas fijan la manera en que la información es reunida, controlada, almacenada, utilizada y divulgada. Por lo general, solamente la información particular es objeto de regulación por el método de protección de datos. Esta información personal o datos personales se explican como la información que posibilitan la identificación de un sujeto, ya sea persona natural o jurídica (nombrados como individuos) o en algunas circunstancias entidades colectivas. El propósito principal de estas medidas es la salvaguarda de los intereses y derechos del individuo en el momento en que información acerca del mismo está siendo manipulada por un tercero. Estos intereses y derechos del individuo se identifican con los conceptos de privacidad, autonomía e integridad.

La Protección de Datos en un mundo cada vez más conectado y complicado identifica una serie de elementos centrales sobre los cuales se establecen todo cuerpo normativo de protección de datos:

1.- La información de carácter personal tiene que estar recogida por medio de medios justos y legales.

2.- La cuantía de datos personales almacenados tiene que estar limitada a lo esencial para satisfacer la necesidad por la que se han recopilado en primera instancia.

3.- La información personal tiene que ser recopilada por fines específicos, legales y legítimas, y no puede de ser procesada de modo contrario a esas finalidades.

4.-La utilización y divulgación de la información personal solo podrá efectuarse para fines que resulten con el permiso de la persona o personas a quien o quienes la información se refiera.

5.- La información personal tiene que ser de carácter relevante, concreta y completa en relación a la finalidad para la que los datos se tratan.

6.- Deben aplicarse medidas de seguridad con la finalidad de salvaguardar dichos datos personales de difusión, destrucción, alteración o uso no autorizados.

7.- Se debe informar a los interesados, además de dar acceso a la información relativa a qué datos personales tienen terceros, así como a permitir rectificar estos datos si son imprecisos o incorrectos.

8.- Los encargados del tratamiento de la información deben responder del desempeño de las leyes que dan resultado a los principios anteriores.

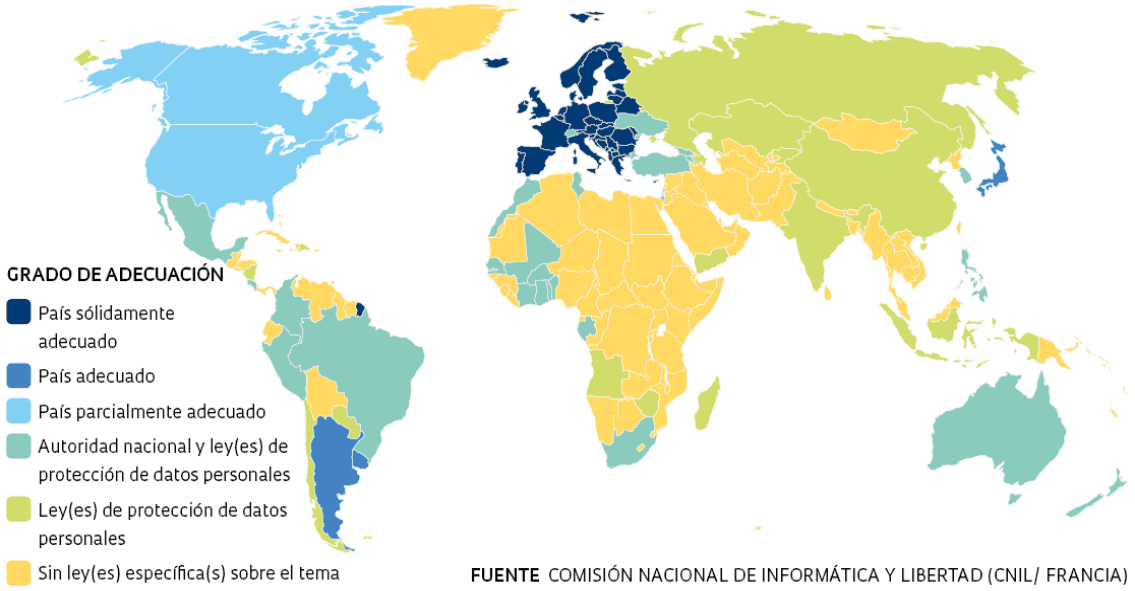
La decisión de la jurisdicción y de la ley aplicable no es el único inconveniente al que nos tenemos que enfrentar. Según las Naciones Unidas, el 66% de los países del mundo poseen una legislación que regularice todo lo relacionado a la protección de datos. Un 10 % cuentan con proyectos de ley referidos a dicha regulación; un 19% no posee una legislación propia para la protección de datos, o esta está sin regular; y un 5% de las naciones del mundo no han proporcionado información al respecto.

No fue hasta la década de los 70 cuando comenzaron a escribirse las primeras partes de lo que hoy es la legislación de protección de datos. Surgieron nuevas herramientas legales y cuasi-legales que conformaron lo que hoy conocemos. Dentro de los primeros instrumentos internacionales, podemos subrayar el Convenio del Consejo de Europa referente a la Protección de los Individuos y respecto del Tratamiento de Datos Personales (acogida en enero de 1981); la Directiva 95/46/CE relativa a la Protección de Personas Físicas en lo referente al Tratamiento de Datos Personales y a la Libre Circulación de los Datos (en vigor desde noviembre de 1995); así como las Directrices de la OCDE basadas en la Protección de la Privacidad y Flujos Transfronterizos de Datos Personales (acogida en septiembre de 1980).

Estas tres herramientas tenían dos propósitos principales: comprendían los elementos primordiales de protección de datos y se utilizaban de modelos para las diferentes iniciativas legislativas que se han llevado a cabo con posterioridad, ya sean nacionales o internacionales. La Protección de Datos en un mundo cada vez más

interconectado y complejo desarrollará con mayor detalle su función antes de la llegada del Reglamento General de Protección de Datos.

Gráfico 6 Legislación en Protección de Datos por países



Fuente: Comisión Nacional de Informática y Libertad.[44]

En el gráfico anterior se muestra un mapa en el que se pueden localizar las distintas regulaciones de protección de datos.

Como ya hemos visto a lo largo de este punto, las tecnologías de la información se han convertido, en cierta manera en un emblema simbólico de la cultura actual. El resultado de esto es el incremento de la preocupación sobre la seguridad de la información y, sobre todo, la información y los datos de carácter personal. La defensa de estos datos es de suma importancia dentro de las múltiples modalidades del *e-commerce* o comercio electrónico, el cual mencionamos anteriormente, y especialmente han supuesto mayor relevancia en el ámbito B2C debido a que los usuarios efectúan transacciones comerciales a través de medios electrónicos, compras en Internet o meramente al intercambiar información y datos personales con otros internautas o empresas.

[44] https://revistapesquisa.fapesp.br/es/con-foco-en-la-privacidad/

6.2.1. Reglamento General de Protección de Datos

Cabe destacar que nuestra presencia en el mundo digital es cada vez más significativa, lo que supone que vamos dejando una cantidad de rastros digitales cada vez más grande a nuestro paso, nuestra identidad digital. Esta identidad digital a la que me refiero es provechosa, por ejemplo, a la hora de realizar gestiones administrativas que precisan identificación y una aprobación específica. De manera simultánea, la existencia de una de estas identidades digitales implica que muchos de nuestros datos personales sean usados, o incluso en ocasiones manipulados o usurpados, por diferentes personas. La privacidad de los datos personales[45] se vuelve una necesidad.

Debido a esto, debemos entender que exista una firme necesidad de consolidar la seguridad en línea y un rendimiento de cuentas para proteger a los usuarios y a la comunidad online de los peligros de una vigilancia generalizada y también concreta, con el fin de impedir que los derechos y libertades fundamentales sean socavados.

Es más, existe un gran debate sobre las expectativas organizativas y tecnológicas para establecer sistemas de identidad digital y carteras personales que obedezcan absolutamente el principio de protección de datos por diseño y por defecto. Un buen ejemplo es la cuestión que los legisladores europeos sostienen actualmente sobre la decisión de instaurar un Marco Europeo de Identidad Digital. El siguiente paso a esto es la creación de un cúmulo de tecnologías y herramientas que favorezcan y apoyen dicho marco.

Para hacer frente a este peligro existente, la Unión Europea ha desarrollado una solución en forma de ley. El Reglamento General de Protección de Datos (RGPD) es el reglamento europeo referente al amparo de las personas físicas en lo que al trato de sus datos personales y a la libre circulación de estos respecta. Entró en vigencia el 24 de mayo de 2016 y fue aplicable a partir del 25 de mayo de 2018, durante dos años empresas, organizaciones, organismos e instituciones fueron adaptándose para su desempeño. Es una normativa a nivel europeo, así que cualquier empresa que pertenezca a la unión, que tengan negocios en la UE o que controlen cualquier tipo de información, deberán aceptarla y cumplirla. Las multas por el incumplimiento de esta normativa pueden llegar a alcanzar hasta los 20 millones de euros.

[45] Datos personales: toda información sobre una persona física identificada o identificable, se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente. https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex%3A32016R0679

En nuestro país el Reglamento General de Protección de Datos dejó sin validez a la Ley Orgánica de Protección de Datos de Carácter Personal (LOPD) del año 1999, siendo reemplazada el 6 de diciembre de 2018 a causa de la Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales, conforme con el nuevo reglamento.

Este marco reglamentario fue la consecuencia de un proceso que comenzó en el año 2010 cuando el Consejo Europeo instó a la Comisión Europea a valorar el funcionamiento de la Unión Europea en cuanto a la protección de datos y a plantear nuevas iniciativas legislativas. Fue en la resolución del Programa de Estocolmo [46] cuando el Parlamento Europeo propuso una postura a favor de la preparación de una normativa renovada, un régimen general para regular la defensa de datos dentro de la Unión Europea. Se necesitaba un marco más amplio, consistente y actualizado a las necesidades y escenario de la protección de datos. Se requería fortalecer la seguridad jurídica de la población europea, operadores económicos y autoridades públicas; igualmente había que evitar la fragmentación en la diligencia de la protección de datos en el entorno personal antes existente.

El 27 de enero de 2012 la Comisión Europea expuso una Propuesta de Reglamento referente a la protección de las personas físicas en lo vinculado al tratamiento de datos personales, también en lo referente a la libre circulación de estos datos. Esta propuesta fue objeto de muchas reformas a lo largo de 3 años, hasta que el 15 de diciembre de 2015 el escrito fue admitido por la Comisión de Libertades Civiles, Justicia y Asuntos de Interior del Parlamento Europeo. El texto legal fue definitivamente publicado en el Diario Oficial de la Unión Europea[47] el 4 de mayo de 2016, bajo el nombre de: Reglamento UE 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, referido a la protección de las personas físicas y al tratamiento de datos personales y libre circulación de estos. Por el que se deroga la Directiva 95/46/CE. Por lo general se le denomina por las siglas RGPD o GDPR (por sus siglas en inglés).

El medio de aplicación del Reglamento General de Protección de Datos se recoge en el artículo 2, en el cual se establece que “El presente Reglamento se aplica al tratamiento total o parcial automatizado de datos personales, así como al tratamiento no automatizado de datos personales comprendidos o predestinados a ser incluidos en un fichero. También

[46] El Programa de Estocolmo fue un programa que establecía un plan de trabajo para el trabajo de la Unión Europea (UE) en el espacio de libertad, seguridad y justicia para el período 2010-2014.
[47] DOUE: L 119, 4.5.2016, p. 1–88 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:02016R0679-20160504

se consideran una serie de supuestos fuera del ámbito de aplicación material, especificándose estas exclusiones para: el ejercicio de actividades no comprendidas en el ámbito de aplicación del Derecho de la Unión Europea; a la actividad de las autoridades con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales, o de ejecución de sanciones penales, además de la protección frente a amenazas a la seguridad pública; las actividades de los Estados Miembros comprendidas en el ámbito de aplicación del capítulo 2 del título V del Tratado de Funcionamiento de la UE; y por último, el tratamiento de datos efectuado por una persona física en el ejercicio de actividades exclusivamente personales o domésticas. Respecto del ámbito de aplicación territorial, éste se recoge en el siguiente artículo. Será de aplicación al tratamiento de datos personales en el contexto de las actividades de un establecimiento del responsable o del encargado en la Unión Europea, independientemente de que el tratamiento tenga lugar en la Unión o no"[48].

Algunas de las exigencias más destacadas para las organizaciones son las valoraciones de impacto sobre la privacidad, la notificación de las brechas de seguridad, el trato de los datos más sensibles y las garantías añadidas para la transmisión internacional de datos. Incumplir estas obligaciones pueden llevar a las empresas a recibir sanciones por parte de los organismos competentes y a pesar de que convendría que todas las organizaciones, empresas y sociedades tuvieran o contaran con los servicios de una entidad especializada en materia de Protección de Datos siguen ocurriendo incumplimientos.

En la actualidad existen tres tipos de sanciones que se clasifican, dependiendo de su gravedad, en leves (sanción de hasta 40 000 euros), graves (sanciones de hasta 300 000 euros) y muy graves (sanciones de hasta 20 000 000 euros).

En nuestro país las multas más comunes de producen a cusa de incumplir con los principios de procesamiento de estos datos, poseer una base encargada de procesar los datos personales insuficiente o poseer medidas tanto técnicas como organizativas de seguridad que no sean suficientes. También son habituales las multas por incumplimiento o cumplimiento escaso de los derechos de los interesados y por el incumplimiento de los deberes de información.

Por otra parte, existen criterios determinados los cuales se deben cumplir para impedir la imposición de sanciones referidas a la vigente normativa. Una de las principales

[48] Artículo 2, apartado primero, segundo y tercero del Reglamento (UE) General de Protección de Datos.

recomendaciones para todas las organizaciones es contar con los servicios de una empresa especializada en Protección de Datos. Este tipo de servicios deberán implicar un análisis o auditoría previa de la compañía para valorar sus necesidades y un servicio permanente de asistencia para corroborar el cumplimiento normativo.

La calidad de este servicio es tan significativa que la Agencia Española de Protección de Datos (AEPD) advierte a pymes y autónomos de los peligros de contratar servicios de adecuación normativa que no tengan costes, con un costo muy bajo o inclusive gratuito. Las sanciones económicas más cuantiosas se han impuesto las grandes compañías reconocidas en todo el territorio español. Sin embargo, todas las organizaciones, sin importar su tamaño o relevancia, son frágiles en este ámbito.

Ante esta situación, una de las sugerencias principales de los expertos es acudir a los servicios de consultoría de protección de datos. Fundamentalmente en los sectores donde la existencia del delegado de Protección de Datos es imperativa, este procedimiento resulta imprescindible. Igualmente, aconsejan a las empresas llevar a cabo auditorías de forma interna, del mismo modo que sugieren desarrollar y actualizar habitualmente los manuales de seguridad en los que se dictaminan las medidas para la protección de datos conformes a la legislación actual.

El RGPD ha ido captando apoyo de negocio de quienes ven esto como una ocasión para perfeccionar su gestión de los datos. Mark Zuckerberg también lo ha calificado como algo que es muy positivo para Internet, y ha reivindicado que se acojan leyes similares al Reglamento General de la Protección de Datos en los EE. UU.. Asociaciones de derechos del consumidor, como es la Organización Europea del Consumidor, se sitúan entre los más recios defensores de la legislación. El activista y fundador del software libre, Richard Stallman, ha halagado algunas propiedades de la RGPD pero pidió seguridades adicionales para evitar que las empresas de tecnología “autoricen su manufacturación”.

Una de las novedades que ha introducido el RGPD es la incorporación del principio de responsabilidad activa[49], lo cual significa que la responsabilidad del tratamiento de datos debe obedecer a los principios que marca el RGPD y estar preparado para demostrar dicho cumplimiento, estas normas consisten en que debe haber licitud, lealtad y transparencia,

[49] AEPD, guías sectoriales “Protección de datos y administración local”. Disponible en http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/2018/Guia_Proteccion_Datos_Administracion_Local.pdf

los datos tienen que estar actualizados y ante todo se da mucho valor al principio de minimización de datos.

7. RECOMENDACIONES

PRIMERA

Nunca dar información por internet: uno de los principales riesgos a los que te puedes enfrentar si cometes este error es que contacte contigo una empresa falsa bien por e-mail o por teléfono para solicitarte información confidencial. En estos casos, saber si el emisor es realmente quien dice ser es relativamente fácil, generalmente las direcciones de correo electrónico presentan variaciones poco fiables en las letras de su dominio. Ejemplo: bancsantand@grupsantander.es

SEGUNDA

Evitar conectarse a redes no autorizadas: aunque no lo creamos este es uno de los mayores errores que cometen los usuarios. Las redes Wifi públicas son un verdadero peligro para tu privacidad. Si te conectas a una red Wifi abierta ya sea desde tu teléfono móvil o desde tu portátil corres el peligro de que tu actividad en Internet, tus contraseñas o tus datos personales sean sustraídos y monitorizados.

TERCERA

Crear contraseñas difíciles de adivinar: uno de los métodos más utilizados por los crackers (delincuente informático que rompe la seguridad de los ordenadores y las redes) para conseguir contraseñas es por medio de lo que se conoce como fuerza bruta. Esto consiste en probar contraseñas hasta dar con la correcta. Además de este método, también cuentan con programas que de manera automática van probando contraseñas.

CUARTA

Utilizar antivirus y cortafuegos: es totalmente necesario contar con los sistemas de seguridad fundamentales para evitar que se infiltren virus en tu ordenador o bien, si ya se han introducido, poder eliminarlos. Por otra parte, el cortafuegos es otra pieza fundamental de la seguridad de tu ordenador. Con el cortafuegos podrás detener ataques provenientes de otros ordenadores desde los que el ciberdelincuente está intentando conectarse a tu ordenador.

QUINTA

La siguiente recomendación que me gustaría aportar es la importancia de la existencia de una Oficina Técnica de Seguridad (OTS), la cual ya poseen algunas empresas, y que tienen el objetivo de mejorar la ciberseguridad de la organización. Así la gestión de la seguridad del negocio no solo da sustento a la detención y al procesamiento de incidentes, sino que también se anticipa a los incidentes potencialmente peligrosos a través del análisis y vigilancia constante de los activos de la empresa.

SEXTA

Como hemos visto a lo largo de este trabajo es muy difícil crear un entorno 100% en cuanto a ciberseguridad en una organización. Es de obligado cumplimiento realizar con cierta periodicidad auditorías que muestren los niveles de seguridad para estar informados de los riesgos que está asumiendo la compañía. Para esto es recomendable tener uno o varios partners para poder descubrir grietas en la seguridad de la empresa que puedan suponer una amenaza.

SÉPTIMA

Desde mi punto de vista la forma más segura de realizar pagos por Internet es través de la app del banco. En este caso, en el momento en el que realizas la compra, llega una notificación a la aplicación móvil del banco a la cual el usuario debe entrar para poder autorizar la compra bien introduciendo la contraseña, la huella digital o en el caso de algunos smartphones a través del reconocimiento facial.

8. Conclusiones

PRIMERA

La transformación digital de la que hemos hablado a lo largo de la primera parte del trabajo plantea unos entornos en las empresas cada vez más grandes, complejos, confusos y, por lo tanto, con un mayor peligro ante los distintos tipos de amenazas como resultado de un entorno cada vez más expuesto al exterior. Por lo tanto, el desarrollo tecnológico en las empresas y en el mercado debe ir de la mano con el crecimiento en ciberseguridad, para así asegurar el buen funcionamiento de los nuevos servicios y activos digitalizados que se agreguen.

SEGUNDA

Nuestra normativa respecto a la protección de datos de carácter personal se ha renovado mucho con el paso de los años, sobre todo debido a la presión que ejerce sobre nosotros la Unión Europea, que es mucho más pionera en este ámbito. La legislación no ha sido de mucha durabilidad en este tema ya que varía al mismo tiempo que nuestra sociedad y que los avances tecnológicos. En la década de los 70, coincidiendo con la llegada del correo electrónico, teníamos una regulación muy primitiva que regulase el ámbito de la protección de datos y sin embargo en la actualidad contamos con normas estatales, Directivas, Reglamentos Europeos, etc.

TERCERA

El derecho de acceso y el derecho de protección de datos a día de hoy son derechos de configuración legal, no son derechos fundamentales, sin embargo, dentro de la evolución social, poco a poco se están convirtiendo en elementos muy importantes debido a que son materias con las que, sin darnos cuenta, trabajamos cada día. Un ejemplo es dar permiso a una *app* de nuestro *smartphone* para manipular nuestros datos, pedimos una recopilación de estos a un órgano de la Administración Pública, etc. Seguramente, en un futuro no muy lejano, el derecho de protección de los datos de carácter personal y el derecho de acceso a la información serán tan esenciales como lo son los derechos fundamentales que conocemos hoy en día.

CUARTA

El Reglamento General de Protección de Datos representa un antes y un después en la protección de datos de carácter personal, más aún tras disputas tan famosas como la multa que impuso la Agencia Española de la Protección de Datos a empresas privadas de gran magnitud como de WhatsApp o Facebook por la transmisión de millones de datos a terceros sin la aprobación de los afectados, en este momento es cuando las personas empiezan a darse cuenta de lo que significa tener control y que exista seguridad sobre sus datos.

QUINTA

Los profesionales de la seguridad de la información deben realizar controles que los ayuden a ser proactivos, revisarlos constantemente, mejorarlos y probarlos, con la finalidad de hacer disminuir al máximo la repercusión que pueda tener que una amenaza o un riesgo

se vuelva una realidad. Es primordial que impliquemos la seguridad desde un inicio, para así poder anticiparse y actuar a tiempo ante un peligro. Contar con planes de actuación para determinados escenarios puede ser lo que marque la diferencia entre afrontar un problema con la mayor brevedad posible o que la empresa desaparezca.

9. Bibliografía

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS: http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/2018/ Guia_Proteccion_Datos_Administracion_Local.pdf

CIBERCRIMENES Y CIBERSEGURIDAD EN ESPAÑA. DATOS ESTADÍSTICOS. PUBLICADO POR ROSA FERNANDEZ. 18 DE SEPTIEMBRE DE 2022: https://es.statista.com/temas/3166/ciberdelitos-en-espana/#topicHeader__wrapper

CIFRAS DEL INE (Instituto Nacional de Estadística), JUNIO DEL 2020: https://www.ine.es/ss/Satellite?L=es_ES&c=INECifrasINE_C&cid=1259952923622&p=1254735116567&pagename=ProductosYServicios%2FINECifrasINE_C%2FPYSDetalleCifrasINE#ancla_1259952923586

COMPRAS ONLINE EN ESPAÑA. OBSERVATORIO NACIONAL DE TECNOLOGÍA Y SOCIEDAD (ONTSI) EDICIÓN 2021: https://www.ontsi.es/sites/ontsi/files/2021-12/informecomprasonlinespa%C3%B1a2021.pdf

CONSEJO EUROPEO. PACTO VERDE EUROPEO: https://www.consilium.europa.eu/es/policies/green-deal/#:~:text=%C2%BFQu%C3%A9%20es%20el%20Pacto%20Verde,clim%C3%A1tica%20de%20aqu%C3%AD%20a%202050.

DIGITALIZAR Y DIGITALIZARSE: LA OPORTUNIDAD DE LAS PYMES. CANAL DE YOUTUBE OFICIAL DEL BANCO BBVA ESPAÑA, 22 DE JUNIO DEL 2022: https://www.youtube.com/watch?v=rjxxNhg3GJA

EL PAÍS. CINCO DÍAS, MARIMAR JIEMENEZ. 7 DE FEBRERO DE 2022: https://cincodias.elpais.com/cincodias/2022/02/07/companias/1644235814_623711.html#:~:text=La%20digitalizaci%C3%B3n%20de%20la%20econom%C3%ADa,digitalizaci%C3%B3n%20generadas%20por%20la%20pandemia.

ESTRATEGIA NACIONAL DE CIBERSEGURIDAD. PÁGINA WEB DEL DEPARTAMENTO DE SEGURIDAD NACIONAL: https://www.dsn.gob.es/es/documento/estrategia-nacional-ciberseguridad-2019

HORIZONTE EUROPA: https://www.horizonteeuropa.es/

MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL. 3 DE AGOSTO DEL 2022: https://portal.mineco.gob.es/es-es/comunicacion/Paginas/retech.aspx

MONCLOA. ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL. INFORMES DESI: https://www.lamoncloa.gob.es/serviciosdeprensa/notasprensa/asuntos-economicos/Paginas/2022/280722-digitalizacion.aspx

ORGANIZACIÓN DE CONSUMIDORES Y USUARIOS. SISTEMAS DE AUTENTICACIÓN REFORZADA. 12 DE ABRIL DE 2021: https://www.ocu.org/dinero/cuenta-bancaria/consejos/sistemas-autenticacion-reforzada#:~:text=Los%20mecanismos%20de%20autenticaci%C3%B3n%20reforzada,%2C%20por%20ejemplo%2C%20una%20contrase%C3%B1a

PANORAMA ACTUAL DE LA CIBERSEGURIDAD EN ESPAÑA. COCKTAIL ANALYSIS: https://www.ospi.es/export/sites/ospi/documents/documentos/Seguridad-y-privacidad/Google_Panorama-actual-de-la-ciberseguridad-en-Espana.pdf

PERIÓDICO ONLINE DE RECURSOS HUMANOS. RRHH DIGITAL. NAGI PEREZ, RESPONSABLE DE UDEMY BUSINESS EN ESPAÑA 20 DE SPETIEMBRE DE 2022: http://www.rrhhdigital.com/editorial/154442/como-garantizar-la-empleabilidad-a-largo-plazo-en-el-mercado-laboral-del-futuro

PORTAL ESTADÍSTICO DE CRIMINALIDAD, MINISTERIO DEL INTERIOR, GOBIERNO DE ESPAÑA: https://estadisticasdecriminalidad.ses.mir.es/publico/portalestadistico/

PROPUESTA DE REGLAMENTO DEL PARLAMENTO EUROPEO Y DEL CONSEJO POR EL QUE SE ESTABLECEN NORMAS ARMONIZADAS EN MATERIA DE INTELIGENCIA ARTIFICIAL (LEY DE INTELIGENCIA ARTIFICIAL): https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex:52021PC0206

PROPUESTA DE REGLAMENTO DEL PARLAMENTO EUROPEO Y DEL CONSEJO RELATIVO A UN MERCADO ÚNICO DE SERVICIOS DIGITALES (LEY DE SERVICIOS DIGITALES): https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:52020PC0825

PROPUESTA DE REGLAMENTO DEL PARLAMENTO EUROPEO Y DEL CONSEJO SOBRE MERCADOS DISPUTABLES Y EQUITATIVOS EN EL SECTOR DIGITAL (LEY DE MERCADOS DIGITALES): https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:52020PC0842

REGLAMNETO RELATIVO A LA PROTECCIÓN DE LAS PERSONAS FÍSICAS EN EL TRATAMIENTO DE DATOS PERSONALES Y A LA LIBRE CIRCULACIÓN DE DATOS: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:02016R0679-20160504

REVISTA DIGITAL BUSINESS INSIDER, ALBERTO R. AGUIAR, 23 DE SEPTIEMBRE DEL 2022: https://www.businessinsider.es/kit-digital-inyectara-300-millones-ciberseguridad-espanola-1128449