Facultad de Ciencias Sociales y Jurídicas

Grado en Derecho

Universidad de Jaén

Facultad de Ciencias Sociales y Jurídicas

Trabajo Fin de Grado

# ALGUNAS CUESTIONES CONTROVERTIDAS EN TORNO AL DERECHO A LA PROTECCIÓN DE DATOS EN EL COMERCIO ELECTRÓNICO

**Ana Negrillo Bueno**

**Enero, 2021**

## RESUMEN

El objeto de este trabajo es indagar sobre los entresijos del comercio electrónico, y más concretamente, de los instrumentos de pago electrónico, en relación con la protección de datos. Tras hacer un repaso a la historia del derecho fundamental a la protección de datos y conocer de manera más profunda el comercio electrónico, se dará paso a una investigación enfocada en la protección de datos en los procesos de pago electrónico mediante tarjetas bancarias. Para ello, se analizarán los datos más vulnerables que se exponen en estos procesos, los riesgos que conlleva la utilización de estos medios de pago, la legislación que protege estos datos y los derechos que tienen los ciudadanos respecto al tratamiento de sus datos. Todo esto con la finalidad de esclarecer las consecuencias que conlleva el comercio electrónico en la protección de datos, y cómo mantener nuestros derechos fundamentales a salvo de cualquier posible intromisión.



**Palabras clave:** protección de datos, Reglamento General de Protección de Datos, derechos fundamentales, privacidad, comercio electrónico, pago electrónico, tarjetas bancarias, seguridad jurídica.

## ABSTRACT

The purpose of this work is to investigate the ins and outs of e-commerce, and specifically, electronic payment instruments, in relation to data protection. After a review of the history of the fundamental right of data protection and a deeper knowledge of e-commerce, we will continue with a research, focusing on data protection in electronic payment processes using bank cards. For that reason, we will analyse which is the most vulnerable data in those bank cards during the payment process, the risks involved in these payment tools, the legislation in charge of the protection of the data exposed and, the rights that citizens have with regard to the processing of their data. All of this will be done with the aim of clarifying the consequences of electronic commerce on data protection and how to keep our fundamental rights save from any possible interference.



**Keywords:** data protection. General Data Protection Regulation, fundamental rights, privacy, e-commerce, electronic payment, bank cards, juridical security.

## ÍNDICE DE CONTENIDOS

## 1. INTRODUCCIÓN.

Es una realidad incuestionable el hecho de que las nuevas tecnologías se han mimetizado por completo en nuestra sociedad, convirtiendo estos continuos cambios en una constante en la vida de las personas. Uno de los hechos más trascendentales de los últimos tiempos ha sido la aparición de *Internet*. La *'World Wide Web'* dio un giro de 360 grados a la forma en la que entendíamos el mundo, revolucionando por completo nuestra vida y, de manera más significante las telecomunicaciones y la economía en general.

*Internet* trajo consigo una nueva forma de comunicación y una nueva perspectiva para el comercio. Las redes sociales y el comercio electrónico han dado un vuelco a las telecomunicaciones y a la economía. A través de las redes sociales podemos comunicarnos de manera rápida y sencilla con personas de cualquier parte del mundo y, con el uso del comercio electrónico ya no es necesario trasladarnos al establecimiento físico para realizar nuestras compras.

Unos cambios muy beneficiosos para todos, pero con los años, han ocasionado un gran problema: la exposición de datos. Cada día hacemos uso de *Internet*, muchas de las actividades que realizamos dependen del mismo y por lo tanto estamos constantemente expuestos al mal uso de los datos personales. Las nuevas herramientas que el progreso tecnológico nos ha brindado se han convertido en un reto para la protección de datos, siendo necesaria una constante actualización en la protección de los datos de las personas.

En el ámbito del comercio electrónico esto no es diferente, con cada compra que llevamos a cabo, una serie de datos de carácter personal empiezan a ponerse en circulación, poniendo en peligro la integridad de nuestros derechos fundamentales, como son la intimidad, la dignidad o el honor, entre otros. Uno de los momentos donde el comprador es más vulnerable es en el proceso de pago en las compras *online*, los sistemas de pago electrónico mediante tarjetas bancarias pueden ocasionar brechas en la seguridad de los datos y vulnerar nuestros derechos como resultado del tratamiento que se da a los datos de pago.

Cada vez es más frecuente la compra por medio del comercio electrónico, España ya cuenta con 22 millones[1] de compradores digitales y con la situación actual en la que nos encontramos por la pandemia, este número irá creciendo como consecuencia de los

[1] Artículo de 'El Economista': *La tendencia en el comercio electrónico la marcarán los 'marketplaces' en 2021* (30 noviembre 2020).

cambios, en favor del comercio electrónico, que se están ocasionando en los comportamientos de compra de los consumidores. Por este motivo es tan importante la existencia de una protección de datos real y efectiva que asegure el total respeto de los derechos de los ciudadanos.

Con la realización de este trabajo mi principal objetivo es esclarecer el tratamiento que se les da a los datos en los procesos de compra del comercio electrónico y de manera más específica, a los datos de las tarjetas bancarias: Cuáles son los datos que se exponen, qué leyes protegen estos datos, a qué riesgos se enfrentan los compradores y cuáles son los derechos que tienen frente al tratamiento de sus datos.

## 2. DERECHO A LA PROTECCIÓN DE DATOS.

### 2.1 ¿Qué es el derecho a la protección de datos?

El derecho a la protección de datos es un derecho fundamental que se encuentra en continua evolución debido a la frecuente aparición de nuevas tecnologías que pueden suponer una exposición pública constante de los datos de las personas. Como derecho fundamental, se encuentra recogido en la Constitución española (CE), más concretamente, en el artículo 18.4 CE en el que se expone que *'la ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos'*. El derecho a la protección de datos no tiene una mención expresa en la Constitución pero el Tribunal Constitucional lo declaró como derecho de carácter autónomo en la Sentencia del Tribunal Constitucional 292/200, de 30 noviembre de 2000[2].

Este derecho fundamental tiene como objetivo principal salvaguardar los datos personales de los sujetos, es decir, aquellos datos que permitan la identificación de una persona, tales como el nombre, los apellidos, dirección de correo electrónico, número del documento nacional de identidad, datos médicos,…etc. En definitiva, cualquier dato que

[2] Sentencia 292/2000, de 30 de noviembre de 2000. Recurso de inconstitucionalidad 1.463/2000. Promovido por el Defensor del Pueblo respecto de los arts. 21.1 y 24.1 y 2 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. Vulneración del derecho fundamental a la protección de datos personales. Nulidad parcial de varios preceptos de la Ley Orgánica. «BOE» núm. 4, de 4 de enero de 2001, páginas 104 a 118 (15 págs.).

identifique a una persona. La Comisión Europea define estos datos personales como aquella información referida a una persona física viva identificada o identificable, también todas las informaciones que una vez recopiladas puedan dar lugar a la identificación de una persona[3].

Por otro lado, a través de este derecho, se le reconoce al ciudadano la facultad de controlar sus datos personales y la capacidad para disponer y decidir sobre los mismos[4]. El sujeto es el que debe tener plena disponibilidad sobre el uso de sus datos y es el que debe dar el consentimiento de su uso por parte de terceros. De esta forma, si fuesen utilizados sin su consentimiento se estaría produciendo una clara vulneración del derecho fundamental.

Como todos los derechos fundamentales, es un derecho que dista mucho de ser un derecho absoluto. Es decir, este derecho cuenta con una serie de limitaciones recogidas en las respectivas leyes.

### 2.2 Origen y evolución del derecho a la protección de datos.

El derecho a la protección de datos está estrechamente relacionado con el concepto de intimidad, de privacidad. Para comenzar a hablar de este derecho hay que remontarse a finales del siglo XIX en Estados Unidos donde aparece el derecho a la intimidad o también llamado *right to privacy,* más concretamente, este concepto de privacidad tiene su origen en un artículo, publicado en 1890 en la revista *HarwardLaw Review,* llamado *'The Right to Privacy'* y escrito por Samuel Warren y Louis Brandeis (dos juristas norteamericanos). Este artículo surge como resultado de una investigación de las respuestas que daba el derecho estadounidense a los actos de intromisión de la prensa escrita en la vida privada de las personas. Esta necesidad de dar respuesta a estas intromisiones tiene su origen en la aparición de nuevas cámaras fotográficas que permitían la realización de fotografías instantáneas sin necesitar un largo período de exposición. Es decir, se podían realizar fotografías sin precisar de la colaboración del individuo y, en consecuencia, ser tomadas sin su consentimiento produciéndose así una intromisión en su vida privada. Como puede observarse, este derecho a la protección de

[3] Comisión Europea, Web oficial de la Unión Europea.
[4] Agencia Española de Protección de datos (2004), *Guía del derecho fundamental a la protección de datos de carácter personal,* p.6.

datos se encuentra en constate evolución por las nuevas tecnologías. El origen de este derecho es un claro ejemplo de cómo la aparición de nuevas tecnologías precisa que se tengan que proteger nuevas esferas de la vida del individuo, en este caso la vida privada.

Más tarde, en la década de los 60 del siglo XX, se produce un nuevo cambio en la estructura del concepto de privacidad o *privacy* con la aparición de las primeras bases de datos electrónicos. Empezó a ser necesaria una mayor preocupación por la protección de la intimidad de las personas debido a los nuevos riesgos y amenazas que, los bancos de datos y en general la informática, suponían para esta privacidad. Es aquí donde otro jurista, en este caso el estadounidense Alan F.Westin, proporciona un concepto actualizado del derecho a la privacidad (*right to privacy*), definiéndolo como *'el derecho de los individuos a controlar la información sobre ellos y a decidir cómo, cuándo y de qué manera se transmite esa información a terceros'*, esta definición se empieza a acercar a lo que hoy conocemos como derecho a la protección de datos donde se le reconoce al sujeto la capacidad plena de disponer de sus datos.

Finalmente, en 1974, se adopta en Estados Unidos el *Privacy Act*, pasando a ser la primera ley dirigida a proteger la información y evitar su uso indebido por parte de las autoridades gubernamentales como consecuencia de un escándalo de espionaje y grabaciones de conversaciones (*Watergate*).

En Europa, los primeros países que incorporaron leyes sobre protección de datos a sus legislaciones fueron aquellos que se encontraban más avanzados en cuanto a tecnologías se refiere, como fueron Suecia y Alemania con la adopción, en 1973 y 1977 respectivamente, de una ley nacional de protección de datos. Más tarde, en 1978 se unió Francia con la ley *'informática y libertad'*. En países como Portugal o Austria, esta ley tuvo rango constitucional desde el inicio, añadiendo a sus legislaciones, en 1976 y 1978 respectivamente, los artículos referidos a este derecho. La finalidad principal de la elaboración de estas leyes no fue impedir el uso de los datos en sí, sino, el uso indebido de los mismos.

Si nos trasladamos a España, el derecho a la protección de datos no está recogido como tal en la Constitución Española sino que se integró en el texto lo que sería el fundamento y el marco de la normativa española en materia de protección de datos. Este se encuentra recogido en el artículo 18.4 CE y, tal y como he citado en el epígrafe anterior, el Tribunal Constitucional fue el encargado de declarar su existencia a través de

la STC 292/2000, de 30 de noviembre de 2000. En esta sentencia se establecieron los caracteres del derecho fundamental a la protección de datos, declarándolo un derecho de carácter autónomo y distinto del derecho a la intimidad personal y familiar. En otros países antes mencionados, el origen del derecho está estrechamente relacionado con la protección de datos de carácter informático mientras que en España, esta sentencia aclara que no solo se protegen los datos de tratamiento informático sino todos los datos de carácter personal.

Por último, las organizaciones internacionales también se hicieron eco de la importancia de la protección de los datos de los individuos durante el siglo XX, siendo en la década de los 80 cuando aparecieron los primeros instrumentos internacionales referidos a este derecho. El Consejo de Europa y la Organización para la Cooperación y el Desarrollo Económico (OCDE) fueron las primeras organizaciones internacionales en incorporar el derecho a la protección de datos.

Como se ha visto en este epígrafe, el derecho a la protección de datos surge hace más de un siglo y su importancia va incrementando con el paso de los años debido a los continuos cambios sociales que provocan la aparición de numerosas fuentes de datos de carácter personal que necesitan ser amparados y protegidos. Sin ir más lejos, la Agencia Española de Protección de Datos, ante la situación actual que estamos viviendo provocada por la pandemia Covid-19, ha tenido que hacer frente a las múltiples consultas que se están produciendo debido a las dudas en el tratamiento de datos sobre personas infectadas por coronavirus y evitar que se generen incumplimientos en la normativa de protección de datos sobre el tratamiento de datos personales relativos a la salud.

### 2.3 Legislación relativa al derecho a la protección de datos.

La importancia de la protección de los datos de carácter personal de los individuos y la aparición del consiguiente derecho a la protección de datos, hizo necesaria su regulación.

Tanto el legislador español como los legisladores europeos han amparado este derecho fundamental a través de dos leyes: la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD) y el Reglamento General de Protección de Datos (RGPD) de la Unión Europea.

En España, tal y como se ha referido en el apartado anterior, el derecho a la protección de datos no aparece de forma expresa en la CE sino que se hace referencia al mismo en su artículo 18.4. Es el Tribunal Constitucional quien lo constituye como derecho de carácter autónomo e independiente a través de la STC 292/2000[5] motivada por el recurso de inconstitucionalidad interpuesto por el Defensor del Pueblo contra varios incisos relativos a la *'Comunicación de datos entre Administraciones Públicas'* que suponían una lesión de los artículos 18.1[6],4[7] y 53.1[8] CE.

### 2.3.1 La Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

La Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD) es la ley que se encarga de regular la protección de datos en el territorio español. Debido a la pertenencia de España en la Unión Europea, esta ley desarrolla el Reglamento de la Unión Europea 2016/679 (Reglamento General de Protección de Datos). Aunque desarrolle este Reglamento, la LOPDGDD también incorpora un Título dedicado a los derechos digitales para garantizar los derechos digitales y regular los derechos de los ciudadanos en esta materia.

El objeto de esta ley se divide principalmente en dos puntos, el primero es que esta ley está subordinada al Reglamento 2016/679 de la UE y por lo tanto el ordenamiento español tiene que adaptarse a lo establecido por la Unión Europea en lo que se refiere al tratamiento de los datos personales y a la circulación de los mismos, completando a la misma vez las disposiciones del Reglamento. El segundo punto en el que se divide el objeto de esta ley es el de garantizar a los ciudadanos sus derechos digitales conforme a lo dispuesto en el artículo 18.4 de la Constitución Española.

---

[5] Sentencia del Tribunal Constitucional 292/2000, de 30 de noviembre.
[6] Artículo 18.1 CE: *'Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen.'*
[7] Artículo 18.4 CE: '*La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos.'*
[8] Artículo 53.1 CE: '*Los derechos y libertades reconocidos en el Capítulo segundo del presente Título vinculan a todos los poderes públicos. Sólo por ley, que en todo caso deberá respetar su contenido esencial, podrá regularse el ejercicio de tales derechos y libertades, que se tutelarán de acuerdo con lo previsto en el artículo 161, 1, a).'*

### 2.3.2 Reglamento General de Protección de Datos de la Unión Europea (RGPD).

El Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos es la norma que regula la protección de datos en el ámbito europeo y que derogó la Directiva 95/46/CE.

La Unión Europea también considera este derecho como fundamental y así lo demuestra al quedar recogido en la Carta de Derechos Fundamentales de la UE donde en su artículo 8[9] defiende que, los ciudadanos de la Unión tienen derecho a que sus datos personales se encuentren debidamente protegidos.

## 2.4 Relación del derecho a la protección de datos con otros derechos fundamentales

A pesar de ser un derecho fundamental de carácter autónomo e independiente del resto de derechos fundamentales, el derecho fundamental a la protección de datos guarda relación con el resto de los derechos fundamentales de la personalidad amparados por la Constitución Española, como serían los recogidos en el primer apartado del artículo 18: *'se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen'.*

### 2.4.1 Derecho a la intimidad.

Existe cierta relación entre los conceptos que forman parte de estos derechos fundamentales y el derecho a la protección de datos, uno de ellos es el concepto de *intimidad*. Este concepto guarda un estrecho vínculo con la protección de datos habida cuenta de que, cuando se produce un uso indebido de los datos de carácter personal del individuo, la intimidad del mismo queda vulnerada. El concepto de intimidad es un

[9] Carta Derechos Fundamentales UE, Artículo 8 relativo a la protección de datos de carácter personal: *'1. Toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan. 2. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que le conciernan y a obtener su rectificación. 3. El respeto de estas normas estará sujeto al control de una autoridad independiente'*

concepto amplio y complejo, no se puede delimitar de manera exacta debido a los constantes cambios que se producen en la sociedad y por tanto con el desarrollo de nuevas tecnologías aparecen nuevos riesgos de intromisión en la esfera íntima y personal del individuo y por consiguiente, nuevos aspectos que deben ser protegidos por este derecho.

En este contexto, es interesante mencionar la *'teoría del mosaico'*[10] para encontrarnos con otro concepto de intimidad que también estaría ligado a la protección de datos. La teoría del mosaico quiere hacer entender la necesidad de proteger la intimidad de las personas frente a la tecnología y más concretamente, la informática, comparando los datos que circulan de los individuos con un mosaico, es decir, cada dato sería una pieza del mosaico que de forma individual no tiene relevancia pero que al unirla con el resto de piezas crea un mosaico integrado por un grupo de datos del individuo que pueden suponer una amenaza para su intimidad, obteniendo una información más completa y por tanto, peligrosa para la integridad de sus derechos. Esta teoría consiste en *"un modelo empleado por los expertos en seguridad para extraer información sobre empresas, que se basa en la combinación de datos públicos con datos privados para extraer del mosaico resultante conclusiones sobre el comportamiento del sujeto analizado"*. Los defensores de esta teoría se apoyan en un enfoque acumulativo de la evaluación de los datos que se han recopilado del sujeto. El peligro reside en la acumulación de datos sobre geolocalización que, de manera aislada son inocuos pero que al visualizarlos globalmente pueden formar pautas de comportamiento del individuo al que pertenezcan los datos de localización examinados. Para que exista un 'mosaico' es necesario que haya un número suficiente de datos que de manera conjunta tengan como resultado un cuadro de hábitos y conductas referidas a un sujeto, permitiendo así la realización de predicciones.[11] El uso del GPS sería un claro ejemplo de la teoría del mosaico: los datos obtenidos por el rastreo de estos dispositivos en un día cualquiera no serían concluyentes pero si este seguimiento fuese continuado en el tiempo, podrían predecirse patrones de comportamiento y características de un sujeto, afectando de manera directa a sus derechos fundamentales. Todos estos avances tecnológicos están en el punto de mira debido a la inferencia que pueden causar en la esfera privada de las personas. Con la protección de los datos

[10] Madrid Conesa, F. (1984). *Derecho a la intimidad, informática y estado de derecho. p. 45*. Valencia: Universidad de Valencia.
[11] Bellovin, S.M, Hutchins, R.M, Jebara, T, Zimmeck, S. (2013). *"When enough is enough: Location Tracking, Mosaic Theory, and Machine Learning", New York University Journal of Law & Liberty.*

informáticos de carácter personal se quieren evitar estas situaciones y por ello el derecho a la intimidad y el derecho a la protección de datos están tan relacionados.

### 2.4.2 Derecho al honor.

Respecto al derecho al honor, la RAE[12] define el derecho al honor como el *'derecho a que se respete la reputación, fama o estimación social de una persona'*. Partiendo de esta base, podemos encontrar el punto de conexión entre el derecho al honor y el derecho a la protección de datos, que sería el quebrantamiento de este derecho en el momento que se hace un uso indebido o un uso no autorizado de unos datos pertenecientes a una persona en concreto. En el momento que se produce esta intromisión ilegítima en la esfera privada del sujeto, se puede producir una vulneración del derecho al honor, es decir, el descubrimiento de los datos puede provocar un perjuicio en la reputación, la fama o la estimación social de la persona en cuestión. Póngase como ejemplo, el aparecer en un registro de morosos o de infractores de tráfico y que este registro sea público y de fácil acceso.

En definitiva, todos estos derechos se encuentran interconectados debido a que son derechos fundamentales referidos a la personalidad del sujeto, es por eso que cualquier vulneración del derecho a la protección de datos va a poder causar daños en otros derechos fundamentales.

## 3. PROTECCIÓN DE DATOS Y COMERCIO ELECTRÓNICO.

### 3.1 El comercio electrónico o *e-commerce*.

El comercio electrónico o también llamado *e-commerce* hace referencia a las compras y a las ventas que se llevan a cabo a través de medios electrónicos, es decir, utilizando *Internet* u otras redes informáticas. Esta forma de comercio se distingue del

[12] Diccionario panhispánico del español jurídico.

comercio tradicional por el uso de tecnologías de la información y comunicación, comúnmente conocidas como 'TIC'[13].

Se trata de la compra y venta tanto de productos, como de servicios o incluso, información, con la peculiaridad de que el contacto físico o la presencia del comprador y el vendedor, no es necesaria. Debido a que se trata de un comercio realizado a través de *Internet*, la adquisición de artículos virtuales como la compra de *software*, accesos a contenidos de páginas *web*, etc., es algo característico y frecuente en el *e-commerce*.

Existen perspectivas diferentes que aportan definiciones alternativas del comercio electrónico:[14]

- Desde la perspectiva de las comunicaciones, se puede definir el comercio electrónico como el traslado de información, productos, servicios o pagos, a través de líneas telefónicas y redes de ordenadores.
- Desde la perspectiva de las empresas, el comercio electrónico consiste en aplicar tecnologías avanzadas a fin de automatizar las transacciones entre las organizaciones.
- Desde la perspectiva de los servicios, es un instrumento que brinda la oportunidad de disminuir los costes e incrementar la calidad y la velocidad de los servicios que se realizan.

Otra definición que aporta la Organización Mundial del Comercio (OMC) es aquella que define al comercio electrónico como '*la producción, publicidad, venta y distribución de productos a través de las redes de telecomunicaciones'.*[15]

El origen del comercio electrónico puede empezar a vislumbrarse en torno a la década de los 70, a pesar de lo que se pueda pensar debido a la novedad que supone el *e-commerce*. Los primeros indicios aparecen con el Intercambio Electrónico de Fondos (EFT) entre entidades financieras, más concretamente, en el año 1979 aparecen estos intercambios en España con motivo del Sistema Nacional de Compensación Bancaria. Posteriormente, en los años 80, se van propagando hasta llegar a las compañías, que hacen

[13] Martín, P., (2018). *Teletrabajo Y Comercio Electrónico*. Madrid: Ministerio de Educación, Cultura y Deporte.
[14] Escobar, E. M. (2000). *El comercio electrónico: perspectiva presente y futura en España*. Madrid: Fundación Retevisión.
[15] Organización Mundial del Comercio (OMC).

uso de estas transacciones electrónicas para el envío de mensajes electrónicos, surgiendo así el Intercambio Electrónico de Datos (EDI) y la mensajería electrónica.[16]

En la década de los 90, esta nueva forma de comercio empieza a aparecer como otra vía de llevar a cabo las distintas transacciones que, hasta ese momento se realizaban de la manera tradicional, es decir, a través de tiendas físicas. Es en 1995 cuando aparecen las que serán las dos empresas precursoras del comercio electrónico: *Amazon* y *eBay*. *Amazon* centraba su negocio en la venta de libros, desarrollándose a gran velocidad mientras que *eBay*, se dedicaba a las subastas por *Internet*.[17]

La OMC en la Declaración sobre el Comercio Electrónico Mundial de 1998 establece un programa para examinar todo lo referente y relacionado con el comercio electrónico mundial que tuviera incidencia sobre el comercio. El 25 de septiembre de 1998 el Consejo General de la OMC adoptó el proyecto para más tarde empezar con las deliberaciones en los distintos consejos que forman la OMC. Los miembros de esta organización pactaron la no aplicación de derechos de aduana a las transmisiones electrónicas.[18]

En los inicios, era patente la cierta desconfianza que generaba el comercio electrónico, pero poco a poco se fueron vislumbrando las numerosas ventajas que podía ofrecer este nuevo sistema de comercio, tanto para los negocios como para los consumidores. De igual forma, los avances que iban apareciendo respecto a *Internet*, tales como la llegada de nuevos motores de búsqueda como *Google*, hicieron que el comercio electrónico fuese ocupando nuevos puestos de popularidad entre empresas y consumidores.

El comercio electrónico al tratarse de una nueva forma de comercio presenta variaciones respecto al comercio tradicional, es por ello que surge la necesidad de elaborar una legislación que regule todos los aspectos que suponen una novedad frente al comercio tradicional.

En España, la ley que se encarga de la regulación del comercio electrónico es la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico. La ley tiene como objeto regular las responsabilidades y las obligaciones de los vendedores y de los prestadores de servicios, al igual que proteger los intereses de los

[16] Escobar, E. M. (2000). *El comercio electrónico: perspectiva presente y futura en España*. Madrid: Fundación Retevisión.
[17] Martín, P., (2018). *Teletrabajo Y Comercio Electrónico*. Madrid: Ministerio de Educación, Cultura y Deporte.
[18] Organización Mundial del Comercio (OMC).

destinatarios de los servicios para que cuenten con las garantías necesarias a la hora de la compra de un bien o la contratación de un servicio.[19]

A través de esta ley, se incorpora al ordenamiento jurídico español la Directiva 2000/31/CE, del Parlamento Europeo y del Consejo, de 8 de junio, relativa al comercio electrónico y, de forma parcial, la Directiva 98/27/CE, del Parlamento Europeo y del Consejo, de 19 de mayo, relativa a las acciones de cesación en materia de protección de los intereses de los consumidores al establecer en el texto de la ley, una acción de cesación contra las conductas que vulneren lo dispuesto en la misma.

Actualmente, el comercio electrónico ha pasado a ser una forma de comercio con gran peso en la economía, facilitando la realización de transacciones tanto dentro de España como aquellas realizadas con el exterior. Los últimos datos[20] que se tienen del número de transacciones de comercio electrónico realizadas y del volumen de negocio son los correspondientes al primer trimestre de 2020, siendo el total del volumen de negocio obtenido por el comercio electrónico 12.243.393.034 euros: 6.215.011.359 euros pertenecen a las transacciones de comercio electrónico realizadas desde España con el exterior, 3.772.831.074 euros corresponden a las transacciones dentro de España y 2.255.550.601 euros forman parte de las transacciones llevadas a cabo desde el exterior con España

Respecto al número de transacciones existentes en el primer trimestre de 2020, el total que se ha registrado ha sido de 226.561.402 transacciones. De esta cantidad, 134.888.963 transacciones corresponden a las transacciones realizadas desde España con el exterior, 73.383.299 corresponden a las realizadas dentro de España y, 18.289.140 son las transacciones de comercio electrónico llevadas a cabo desde el exterior con España.

Como se puede observar a través de estas cifras, se realizan millones de transacciones en cuestión de meses provocando la aparición de un gran flujo de datos electrónicos que viajan constantemente de un lugar a otro. Es por ese motivo que, con la aparición de esta nueva forma de comercio, la importancia de la protección de datos se ha visto potenciada. Cantidades inimaginables de datos van circulando por la red, siendo muchos de ellos de carácter personal y por lo tanto, susceptibles de ser una amenaza para los derechos fundamentales de los consumidores.

[19] Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.
[20] Comisión Nacional de los Mercados y la Competencia.

Los instrumentos electrónicos de pago son fundamentales para el desarrollo del comercio electrónico puesto que, una de las ventajas del comercio electrónico es la facilidad de llevar a cabo la transacción sin necesidad de desplazarse al establecimiento físico y por tanto, hacer efectiva la compra de manera telemática, incluidos los pagos a efectuar por el comprador.

Estos medios electrónicos alcanzan tal trascendencia a causa del vínculo que se crea entre los operadores de telecomunicaciones[21] y entre las entidades financieras, con el fin de crear medios de pago concretos para permitir el desarrollo de este tipo de contratación electrónica como es el comercio electrónico, que se produce sin la presencia simultánea de las partes participantes en el contrato.

El pago a través del comercio electrónico o pago electrónico se define como *'todas aquellas operaciones de pago efectuado con una tarjeta de pista magnética o con un microprocesador incorporado, en un equipo Terminal de Pago Electrónico (TPE) o Terminal de Punto de Venta'.*[22] De esta manera, se estaría cumpliendo con la obligación de pago típica de un contrato mercantil de compraventa pero, a través de medios electrónicos.

La existencia de estos novedosos medios de pago, puede traer consigo la aparición de riesgos para los consumidores, como puede ser la utilización fraudulenta de los mismos o la sustracción de datos personales y de datos bancarios. Por esta razón, es indispensable que exista una protección de estos datos y, que de los medios de pago electrónicos se desprendan una serie de derechos y deberes tanto para el comprador como para el vendedor y para aquel que se encargue del tratamiento de los datos de pago.

Tal y como he mencionado con anterioridad, los avances que se han generado con la llegada del comercio electrónico, han propiciado la creación de varias modalidades de pago electrónico. Se pueden clasificar en dos grupos:[23]

---

[21] Domingos Sanca, F. (2013). *Comercio electrónico y pago mediante tarjeta de crédito en el ordenamiento jurídico español: una propuesta para su implementación en el ordenamiento jurídico de Guinea-Bissau.* Universidad Carlos III, Madrid.

[22] Artículo 1 de la Recomendación 87/589/CEE de la Comisión, de 8 de diciembre de 1987, sobre el Código Europeo de Buena Conducta.

[23] Domingos Sanca, F. (2013). *Comercio electrónico y pago mediante tarjeta de crédito en el ordenamiento jurídico español: una propuesta para su implementación en el ordenamiento jurídico de Guinea-Bissau.* Universidad Carlos III, Madrid.

A) Medios de pago tradicionales.

Los medios de pago tradicionales hacen referencia a aquellos instrumentos que no precisan de medios electrónicos para funcionar, como por ejemplo, dinero en efectivo, el pago contra-reembolso, el cheque, la letra de cambio, pagaré o el giro postal. No son muy frecuentes en el comercio electrónico pero se puede hacer uso de ellos si el vendedor así lo contempla. También se consideran pagos tradicionales las tarjetas bancarias (crédito o débito) y la transferencia bancaria. Estos dos últimos son los medios más empleados por los consumidores para el pago y por ello serán objeto de estudio más adelante haciendo hincapié en la protección de los datos que se generan a través del pago con tarjetas de crédito o de débito.

B) Medios de pago electrónicos.

En este segundo grupo, se encuentran los medios de pago específicos del comercio electrónico, como son los cheques electrónicos, las transferencias electrónicas de fondos, las tarjetas monedero, los medios de pago a través de dispositivos móviles o el dinero electrónico.

### 3.2 Las tarjetas bancarias.

De entre todas las formas de pago electrónico mencionadas en el apartado anterior, se va a hacer un análisis más exhaustivo de las tarjetas bancarias (tanto de crédito como de débito) desde una perspectiva de la protección de datos puesto que, es un medio de pago en el que intervienen datos trascendentales de carácter personal y por tanto, objeto de protección.

Las tarjetas de crédito y las tarjetas de débito han pasado a ser los medios más empleados por los consumidores a la hora de realizar un pago a través de *Internet*. El estudio anual[24] sobre comercio electrónico realizado por el Observatorio Nacional de las Telecomunicaciones y de la Sociedad de la Información (ONTSI) muestra que un 85,2%

[24] Observatorio Nacional de las Telecomunicaciones y de la Sociedad de la Información (ONTSI), *El comercio electrónico B2C en España 2019 (Edición 2020).*

de los compradores opta por el uso de tarjetas de crédito o de débito como forma de pago en las compras a través de *Internet*.

Son un instrumento de pago que se caracteriza principalmente por usar un soporte físico como es la tarjeta en sí, bien es cierto que, en la actualidad existe la posibilidad de contar con la tarjeta bancaria a través de un dispositivo móvil sin necesidad de presentar la tarjeta física.

Dentro de las tarjetas bancarias podemos encontrar principalmente dos tipos: las tarjetas de crédito y las tarjetas de débito. La RAE define las tarjetas de crédito[25] como aquella *'tarjeta electrónica emitida por bancos, grandes almacenes y otras entidades, que permite a su titular el pago sin dinero en efectivo o el acceso al cajero automático'*; mientras que define a las tarjetas de débito[26] como aquella *'tarjeta electrónica mediante la cual el importe de la operación realizada con ella se carga inmediatamente en la cuenta bancaria del titular'.* Ambos tipos de tarjetas son muy similares, diferenciándose solo en el cargo de los pagos, es decir, en las tarjetas de débito el pago recae sobre el dinero disponible en la cuenta del sujeto sin sobrepasar el límite de la misma, mientras que en las tarjetas de crédito, este límite sí puede ser superado contrayendo el titular en ese momento una deuda con el banco por los fondos utilizados.

En vista del peso que las tarjetas bancarias tienen en la sociedad actual, es imprescindible proporcionar a las relaciones contractuales derivadas del comercio electrónico, una seguridad que genere confianza en los usuarios a la vez que se protegen sus derechos fundamentales. Por este motivo, los poderes públicos se han enfrentado al comercio electrónico mediante varios enfoques con el fin de alcanzar este mayor nivel de seguridad y confianza en el comprador. Uno de los enfoques es el referido a la protección de los datos personales de los consumidores como consecuencia de la incidencia de este derecho fundamental en las transacciones de comercio electrónico y, para conseguir que estas transacciones siempre se encuentren dentro de la legalidad y del respeto a los derechos de los compradores.[27]

[25] Real Academia Española.
[26] Real Academia Española.
[27] Aliño Sehwerert, J., (2018). *La protección del consumidor digital: los datos personales en el comercio electrónico*. Revista Jurídica sobre Consumidores y Usuarios., 3, pp.97-115.

### 3.2.1 Protección de datos en el pago electrónico con tarjetas bancarias.

En el momento en el que se procede al pago en una transacción de comercio electrónico, exponemos una serie de datos de carácter más vulnerable que intervienen en el proceso de compra: los datos de las tarjetas bancarias. Son datos de naturaleza sensible puesto que su uso ilícito afecta directamente a la esfera económica de las personas y por tanto requieren una protección adecuada y efectiva. Los datos recogidos en ellas y que necesitan de una especial protección son:

- El PIN de la tarjeta de crédito o de débito.

El PIN es el número de identificación personal del usuario de la tarjeta y está compuesto por una clave de cuatro dígitos que permite la identificación y la realización de ciertas transacciones, como sacar dinero de un cajero automático.

- El PAN o número de la tarjeta de crédito o débito.

Literalmente significa '*Personal Account Number'*, se trata del número que aparece en el anverso de la tarjeta y consta de dieciséis dígitos. Este número es el que se requiere a la hora de realizar el pago electrónico.

- La fecha de caducidad de la tarjeta.

Es el periodo de validez con el que cuenta la tarjeta, es decir, la fecha de expiración de la misma. Se encuentra en el anverso de la tarjeta.

- El número de seguridad de la tarjeta o CVV.

Este número se encuentra en el reverso de la tarjeta y sus siglas significan *'Card Verification Value'.* Como su propio nombre indica, es un código de verificación de la tarjeta que confirma que la persona que está utilizando la tarjeta la tiene en su poder. Este número suele ser solicitado en la realización de una compra *online* para evitar usos fraudulentos de la tarjeta por parte de otra persona distinta al dueño de la misma.

- El número de cuenta bancaria.

Es el número de cuenta al que está asociada la tarjeta de crédito o de débito aunque, no suele ser usado en las compras *online*.

- El nombre y apellidos del titular de la tarjeta.

En el anverso de la tarjeta aparece el nombre y los apellidos del titular, datos que también se piden al formalizar la compra y al ser datos de carácter personal, también tienen que ser protegidos.

A pesar de que el desarrollo del comercio electrónico y su presencia en el día a día de la sociedad es más que palpable, es también evidente la desconfianza que genera el momento de la realización del pago en los compradores. Proporcionar los datos de las tarjetas de crédito o de débito para completar la compra suele suscitar dudas acerca de la seguridad del proceso y del tratamiento que posteriormente se le da a los datos de las tarjetas.

Para cumplir con la normativa vigente sobre protección de datos, los sitios *webs* tienen que informar sobre quién es el responsable del tratamiento de los datos, la finalidad que se le va a dar a los datos, la legitimación, los destinatarios de los datos, los derechos que tienen respecto a sus propios datos, información sobre las *'cookies',* etc., con el fin de dar a las transacciones la legalidad y la seguridad que se requiere.

La Agencia Española de Protección de Datos considera que, la compra *online* a través de tarjetas bancarias, es un sistema de pago seguro aunque conlleve el intercambio *online* de datos bancarios[28]. Esta seguridad radica en la presencia de las llamadas pasarelas de pago en las tiendas *online*. Las pasarelas de pago[29] son un servicio que, incorporado a las tiendas *online*, facilitan el pago por parte de los compradores. La pasarela de pago, se encarga de autorizar el pago con tarjeta, protegiendo los datos de la misma mediante el cifrado de los datos confidenciales, permitiendo la seguridad en la transmisión de la información entre el comprador y el vendedor. Este servicio suele ser ofrecido por los bancos, que serán los que tendrán que verificar la información de pago

[28] Agencia Española de Protección de Datos: *Compra segura en Internet. Guía Práctica.*
[29] Urbano Mateos, S., (2016). *Qué es y cómo funciona la pasarela de pago en ecommerce*. Blog: *Actualidad E-commerce.*

proporcionada, a la misma vez que protegen los datos del cliente. Mediante estas pasarelas de pago, el establecimiento *online* no llega a disponer en ningún momento de los datos de las tarjetas de sus compradores, lo que se traduce en una mayor seguridad en las transacciones. Básicamente, la pasarela de pagos en un comercio electrónico es como el sistema TPV[30] de una tienda física. En los casos donde la tienda no haga uso de las pasarelas de pago, la información recaerá directamente sobre la tienda *online*, que será quien se encargue de la protección de los datos a través de los instrumentos que posea. Por lo que, la seguridad podría verse mermada en consecuencia de la ausencia de una pasarela de pago.

La seguridad en los procesos de pago y en general, en el comercio electrónico, goza de gran importancia y es por ello que en el artículo 82 de la Ley de Protección de Datos se recoge el derecho a la seguridad digital: '*Los usuarios tienen derecho a la seguridad de las comunicaciones que transmitan y reciban a través de Internet. Los proveedores de servicios de Internet informarán a los usuarios de sus derechos'*.

A través de la Ley 16/2009, de 13 de noviembre, de Servicios de Pago, se traspone al ordenamiento español la Directiva 2007/64/CE, del Parlamento Europeo y del Consejo, de 13 de noviembre de 2007, sobre servicios de pago en el mercado interior. En esta ley se hace referencia al tratamiento de los datos relativos a los servicios de pago, más concretamente en el artículo 49. El apartado primero[31] de este artículo, expone que todo lo referente al tratamiento y la cesión de los datos que intervienen en los procesos de pago están sujetos a la Ley de Protección de Datos de Carácter Personal mencionada con anterioridad. El apartado segundo[32] hace mención al consentimiento del sujeto para el tratamiento de los datos de pago, estableciendo que no será necesario este consentimiento cuando los datos que estén usando los sistemas de pago y los proveedores de servicios sean los indispensables para garantizar la prevención, investigación y descubrimiento del

[30] El banco BBVA define el TPV o Terminal Punto de Venta como un dispositivo utilizado en los establecimientos comerciales para llevar a cabo las gestiones de venta, como los cobros con tarjetas bancarias.

[31] Ley 16/2009, de 13 de noviembre, de Servicios de Pago. Artículo 49.1: *El tratamiento y cesión de los datos relacionados con las actividades a las que se refiere la presente Ley se encuentran sometidos a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.*

[32] Ley 16/2009, de 13 de noviembre, de Servicios de Pago. Artículo 49.2 (párrafo primero): *No será necesario el consentimiento del interesado para el tratamiento por parte de los sistemas de pago y los proveedores de servicios de pago de los datos de carácter personal que resulten necesarios para garantizar la prevención, investigación y descubrimiento del fraude en los pagos.*

fraude en los pagos. Además, añade en el segundo párrafo[33], que los sistemas de pago y los proveedores de servicios tendrán autorización para el intercambio de esta información siempre y cuando sea para la consecución de los fines anteriormente citados. Por último, el apartado tercero[34] del presente artículo establece que no será necesario comunicar al interesado, del tratamiento y la cesión de los datos de los que trata el apartado segundo, es decir, aquellos datos estrictamente necesarios para garantizar la seguridad del sistema de pago.

En el ámbito europeo, la Directiva (UE) 2015/2366 del Parlamento Europeo y del Consejo de 25 de noviembre de 2015 sobre servicios de pago en el mercado interior, hace mención a la protección de datos de los sistemas de pago en su artículo 94[35]. Este marco europeo se encuentra incorporado de forma parcial a nuestro ordenamiento mediante el Real Decreto-ley 19/2018, de 23 de noviembre, de servicios de pago y otras medidas urgentes en materia financiera y, tiene como objetivos *'facilitar y mejorar la seguridad en el uso de sistemas de pago a través de Internet, reforzar el nivel de protección al usuario contra fraudes y abusos potenciales, respecto del previsto en la Ley 16/2009, de 13 de noviembre, así como promover la innovación en los servicios de pago a través del móvil y de Internet'.*[36] Respecto a la protección de datos, el artículo 65[37] de dicho Real Decreto remite la protección de los datos de los sistemas de pago a lo establecido por el

[33] Ley 16/2009, de 13 de noviembre, de Servicios de Pago. Artículo 49.2 (párrafo segundo): *Asimismo, los sujetos a los que se refiere el párrafo anterior podrán intercambiar entre sí, sin precisar el consentimiento del interesado, la información que resulte necesaria para el cumplimiento de los citados fines.*

[34] Ley 16/2009, de 13 de noviembre, de Servicios de Pago. Artículo 49.3: *De conformidad con lo dispuesto en el artículo 5.5 de la Ley Orgánica 15/1999, no será preciso informar al afectado acerca del tratamiento y las cesiones de datos a las que se refiere el apartado anterior.*

[35] Directiva (UE) 2015/2366. Artículo 94: *1. Los Estados miembros autorizarán el tratamiento de datos personales por los sistemas de pago y los proveedores de servicios de pago cuando sea necesario a fin de garantizar la prevención, la investigación y el descubrimiento del fraude en los pagos. La facilitación de información a las personas sobre el tratamiento de los datos personales y el tratamiento de dichos datos personales y cualquier otro tratamiento de datos personales a los fines de lo dispuesto en la presente Directiva se llevarán a cabo de conformidad con la Directiva 95/46/CE, con las normas nacionales de transposición de dicha Directiva y con el Reglamento (CE) nº 45/2001.*
*2. Los proveedores de servicios de pago únicamente obtendrán, tratarán y conservarán los datos personales necesarios para la provisión de sus servicios de pago, únicamente con el consentimiento expreso del usuario del servicio de pago.*

[36] Real Decreto-ley 19/2018, de 23 de noviembre, de servicios de pago y otras medidas urgentes en materia financiera (pág. 2).

[37] Real Decreto-ley 19/2018, de 23 de noviembre, de servicios de pago y otras medidas urgentes en materia financiera. Artículo 65: *El tratamiento y cesión de los datos relacionados con las actividades a las que se refiere este real decreto-ley se encuentran sometidos a lo dispuesto en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE y en la normativa española de protección de datos, y en la normativa nacional que lo desarrolla.*

Reglamento (UE) 2016/679, por la normativa española de protección de datos y por la normativa nacional que lo desarrolla.

En el caso de los números de las tarjetas de crédito o débito, son datos de carácter personal y por tanto sujetos a lo establecido en la LOPD, que no requieren el consentimiento del sujeto puesto que es un dato necesario para formalizar el contrato entre comprador y vendedor. Estos datos dejarán de ser utilizados cuando ya no sean necesarios y en ese instante serán cancelados, según establece como regla general la LOPD. La conservación de los datos va a variar según la empresa con la que se esté produciendo esa relación contractual de compra, es decir, los datos se tendrán que conservar durante el tiempo requerido para que se pueda producir la distribución del producto y para poder realizar el cargo en la cuenta del comprador. Cuando la relación contractual haya finalizado, estos datos no podrán emplearse para otro fin. En este contexto, cabe mencionar el principio del plazo de conservación o también llamado principio de limitación del plazo de conservación, que se encuentra plasmado en el artículo 5 del RGPD[38]. Este principio viene a decir que los datos solo serán conservados por el plazo estrictamente necesario para que se produzca la consecución del fin, en este caso, cuando finalice el proceso de compra. Los datos podrán conservarse durante más tiempo siempre y cuando se trate de fines de archivo de interés público, fines de investigación científica, histórica o para fines estadísticos.

Por otro lado, también es necesario hacer referencia al principio de integridad y seguridad o confidencialidad recogido en el apartado f) del artículo 5[39]. Para que no se produzca una vulneración de este principio, los datos tienen que ser tratados de tal forma que pueda hacerse efectiva una apropiada seguridad y protección para evitar el tratamiento no autorizado de los datos, para evitar su pérdida, destrucción o cualquier daño.

[38] Reglamento (UE) 2016/679. Artículo 5.1 e): *mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento de los datos personales; los datos personales podrán conservarse durante períodos más largos siempre que se traten exclusivamente con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, sin perjuicio de la aplicación de las medidas técnicas y organizativas apropiadas que impone el presente Reglamento a fin de proteger los derechos y libertades del interesado («limitación del plazo de conservación»).*

[39] Reglamento (UE) 2016/679. Artículo 5.1 f): *tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas («integridad y confidencialidad»).*

Del respeto de estos principios deben ocuparse las partes que intervienen en el uso de las tarjetas bancarias y los encargados del tratamiento de los datos de las mismas. Se pueden distinguir una serie de sujetos[40] entre los que destacan los tres siguientes:

1 Entidad emisora de la tarjeta.

La entidad emisora de la tarjeta es la entidad de crédito que se encarga de conceder, al cliente, una tarjeta de pago, generalmente de crédito o de débito.[41] Lo más frecuente es que los emisores sean bancos u otras entidades financieras.

2 Titular de la tarjeta.

El titular de la tarjeta es la persona que posee una cuenta de crédito o de débito y a cuyo nombre se crea la tarjeta. Es necesario que se acepte una solicitud para que se pueda conceder la tarjeta al cliente.

3 Proveedor de servicios de pago.

Los proveedores de servicios de pago son las empresas o entidades que asumen la tarea de integrar los sistemas de pago en los comercios electrónicos. Existen múltiples empresas proveedoras de servicios de pago como por ejemplo: *MasterCard*, VISA, *American Express* y *PayPal*, entre otras. La figura del proveedor de servicios de pago tiene un papel de especial trascendencia en los procesos de pago ya que se configuran como los intermediarios entre la empresa de comercio electrónico y los bancos. Procesan el pago *online* suministrando la tecnología necesaria para llevar a cabo el movimiento de dinero de la cuenta bancaria del comprador a la cuenta del comercio *online*.

La Directiva (UE) 2015/2366 en el apartado segundo del artículo 94 hace mención al tratamiento de los datos de las tarjetas bancarias por parte de estos sujetos estableciendo que *'los proveedores de servicios de pago únicamente obtendrán, tratarán y conservarán los datos personales necesarios para la provisión de sus servicios de pago, únicamente*

[40] Domingos Sanca, F. (2013). *Comercio electrónico y pago mediante tarjeta de crédito en el ordenamiento jurídico español: una propuesta para su implementación en el ordenamiento jurídico de Guinea-Bissau.* Universidad Carlos III, Madrid.
[41] Eleconomista.es. (2020). *Entidad Emisora: Qué Es - Diccionario De Economía*.

*con el consentimiento expreso del usuario del servicio de pago'.* Además, los proveedores de servicios de pago tienen una serie de obligaciones que se encuentran recogidas en el artículo 42[42] del Real Decreto-ley de servicios de pago y son las siguientes:

- El proveedor de servicios tiene que asegurarse de que las credenciales de seguridad personalizadas del instrumento de pago solo van a ser accesibles para el usuario de servicios de pago autorizado para el uso del instrumento de pago.
- No podrá enviar instrumentos de pago que no hayan sido previamente solicitados.
- Tendrá que cerciorarse de la disponibilidad de los medios adecuados y gratuitos para que el usuario de los servicios de pago pueda llevar a cabo una notificación o la solicitud de un desbloqueo.
- Proporcionar la posibilidad al usuario de servicios de pago de realizar una notificación con carácter gratuito.
- Una vez realizada la notificación, evitará una utilización posterior del instrumento de pago.
- Por último, el proveedor de servicios se encargará de soportar cualquier riesgo que pueda surgir del envío de un instrumento de pago al usuario de servicios

[42] Real Decreto-ley 19/2018, de 23 de noviembre, de servicios de pago y otras medidas urgentes en materia financiera. Artículo 42: 1. *El proveedor de servicios de pago emisor de un instrumento de pago:*
*a) Se cerciorará de que las credenciales de seguridad personalizadas del instrumento de pago solo sean accesibles para el usuario de servicios de pago facultado para utilizar dicho instrumento, sin perjuicio de las obligaciones que incumben al usuario de servicios de pago con arreglo al artículo 41.*
*b) Se abstendrá de enviar instrumentos de pago que no hayan sido solicitados, salvo en caso de que deba sustituirse un instrumento de pago ya entregado al usuario de servicios de pago.*
*Esta sustitución podrá venir motivada por la incorporación al instrumento de pago de nuevas funcionalidades, no expresamente solicitadas por el usuario, siempre que en el contrato marco se hubiera previsto tal posibilidad y la sustitución se realice con carácter gratuito para el cliente.*
*c) Garantizará que en todo momento estén disponibles medios adecuados y gratuitos que permitan al usuario de servicios de pago efectuar una notificación en virtud del artículo 41.b), o solicitar un desbloqueo con arreglo a lo dispuesto en el artículo 40.4. A este respecto, el proveedor de servicios de pago facilitará, también gratuitamente, al usuario de dichos servicios, cuando éste se lo requiera, medios tales que le permitan demostrar que ha efectuado dicha comunicación, durante los 18 meses siguientes a la misma.*
*d) Ofrecerá al usuario de servicios de pago la posibilidad de efectuar una notificación en virtud del artículo 41.b), gratuitamente y cobrar, si acaso, únicamente los costes de sustitución directamente imputables al instrumento de pago.*
*e) Impedirá cualquier utilización del instrumento de pago una vez efectuada la notificación en virtud del artículo 41.b).*
*2. El proveedor de servicios de pago soportará los riesgos derivados del envío de un instrumento de pago al usuario de servicios de pago o del envío de cualesquiera elementos de seguridad personalizados del mismo.*

de pago o de cualquiera de los elementos de seguridad personalizados que intervengan en el proceso.

### 3.2.2 Derechos de los titulares de las tarjetas bancarias respecto al tratamiento de sus datos.

Como ha sido mencionado al inicio del epígrafe anterior, los datos de las tarjetas bancarias son datos de carácter personal y por tanto regulados por la Ley de Protección de Datos, en consecuencia, los derechos que tienen los titulares de las tarjetas serían los contemplados en esta ley, que también aparecen recogidos en el Reglamento General de Protección de Datos de la UE:

- Derecho de acceso.[43]

Consiste en la posibilidad de dirigirse al responsable del tratamiento de los datos para saber si se están tratando o no los datos de carácter personal del sujeto interesado. En caso afirmativo se podrá obtener información sobre los fines del tratamiento, obtener una copia de los datos objeto de tratamiento, información sobre la categoría en la que se encuentren, los destinatarios de los datos comunicados, el plazo de conservación de los datos, etc.

- Derecho de rectificación.[44]

Es aquel que permite rectificar los datos personales que sean inexactos y completar los datos que se encuentren incompletos. Para poder ejercer este derecho, se precisa de una solicitud donde se incluyan los datos que se quieren rectificar y la modificación que se tenga que llevar a cabo.

[43] Artículo 15 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016.
[44] Artículo 16 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016.

- Derecho de supresión (derecho al olvido).[45]

Se podrá solicitar la eliminación de los datos de carácter personal cuando los datos ya no sean necesarios para los fines con los que se recogieron, cuando se retire el consentimiento, por la oposición al tratamiento de los datos, si los datos fueron tratados de manera ilegal, si los datos requieren ser eliminados para el cumplimiento de una obligación de Derecho de la Unión o de los Estados miembros y cuando los datos se hayan obtenido a través de la oferta de servicios de la sociedad de la información. Este derecho es llamado también derecho al olvido debido a que el responsable del tratamiento de los datos tendrá que comunicar a todo aquel que esté tratando los datos la obligación de suprimir todo lo referido a los mismos. El derecho de supresión no es un derecho ilimitado puesto que puede producirse el caso en el que no se pueda llevar a cabo la supresión de los datos por vulnerar la libertad de expresión e información.[46]

- Derecho a la limitación del tratamiento.[47]

Como su propio nombre indica, este derecho permite la limitación del tratamiento de los datos de carácter personal del interesado, pudiendo suspender el tratamiento de los datos o la limitación del uso de los mismos.

- Derecho a la portabilidad de los datos.[48]

Mediante este derecho, el titular de los datos tiene el derecho de recibir sus datos de carácter personal en un formato estructurado, de uso común y lectura mecánica para, posteriormente, poder transmitirlos a otro responsable del tratamiento si así lo estima oportuno.

[45] Artículo 17 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016.
[46] Agencia Española de Protección de Datos.
[47] Artículo 18 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016.
[48] Artículo 20 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016.

- Derecho de oposición.[49]

Consiste en la capacidad que se le otorga al sujeto para poder oponerse al tratamiento de sus datos personales cuando sean objeto de una misión de interés público o cuando el tratamiento tenga como finalidad la mercadotecnia[50] directa.

- Derecho a no ser objeto de decisiones individualizadas.[51]

Se contempla el derecho del interesado a no ser objeto de la creación de perfiles que puedan provocar decisiones basadas en el tratamiento de los datos y producir efectos jurídicos sobre el sujeto.

## 4. RIESGOS DERIVADOS DEL PAGO ELECTRÓNICO A TRAVÉS DE TARJETAS BANCARIAS.

El creciente desarrollo del comercio electrónico y la proliferación de los medios de pago electrónicos han tenido como resultado la aparición de conductas fraudulentas vinculadas a la utilización de los instrumentos de pago electrónicos, especialmente relacionadas con el uso de las tarjetas bancarias.[52] Estos riesgos provocan una reacción negativa en los consumidores y una desconfianza en los medios de pago electrónico, siendo un obstáculo tanto para los nuevos sistemas de pago como para el propio comercio electrónico.[53]

Los delitos informáticos se definen en la doctrina española como *'aquellas conductas que ponen en peligro o lesionan la integridad, confidencialidad y/o disponibilidad de los datos y sistemas informáticos, sin perjuicio de que además puedan suponer una puesta*

[49] Artículo 21 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016.
[50] La RAE define la mercadotecnia como el *'conjunto de principios y prácticas que buscan el aumento del comercio, especialmente de la demanda'.*
[51] Artículo 22 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016.
[52] Rico Carrillo, M., (2013). *Los desafíos del derecho penal frente a los delitos informáticos y otras conductas fraudulentas en los medios de pago electrónicos.* Ius: Revista Del Instituto De Ciencias Jurídicas De Puebla, nº 31, pp. 207-222.
[53] Domingos Sanca, F. (2013). *Comercio electrónico y pago mediante tarjeta de crédito en el ordenamiento jurídico español: una propuesta para su implementación en el ordenamiento jurídico de Guinea-Bissau.* Universidad Carlos III, Madrid.

*en peligro o lesión de bienes jurídicos distintos'*[54]. Se encuentran tipificados en el Código Penal pero, la gran variedad de conductas, ha complicado la tarea de enmarcar estas nuevas acciones en los tipos penales ya existentes. Con la reforma llevaba a cabo en 2010 y 2015 se han tipificado nuevos supuestos relacionados con el uso de instrumentos de pago. Se podría decir que el bien jurídico que se protege en este tipo de delitos es estrictamente informático, se quiere proteger la integridad y la confidencialidad de los datos, así como de los sistemas informáticos.

Las conductas más comunes relativas a las tarjetas bancarias son la clonación de tarjetas, la falsificación, o las estafas.

La clonación de tarjetas no es un delito que se suela dar en el comercio electrónico sino que ocurre de manera más frecuente en comercios tradicionales o cajeros automáticos, donde mediante un dispositivo electrónico se realiza la copia de los datos de la banda magnética de la tarjeta para crear una reproducción exacta de la tarjeta original y posteriormente hacer un uso fraudulento de la misma. La clonación ha dado lugar al término '*skimming'* para hacer referencia al robo de información de tarjetas como consecuencia del uso legítimo de este medio de pago. En el Código Penal este delito se encuentra recogido en el artículo 399 *bis*[55] que castiga tanto la alteración, copia, reproducción o cualquier tipo de falsificación, como la tenencia de estas falsificaciones o el uso de las tarjetas clonadas.

La clonación de tarjetas bancarias tiene como resultado la falsificación de las mismas, pero también se puede cometer una falsificación de tarjetas sin la realización de una clonación, es decir, elaborando un nuevo instrumento de pago ilícito, obteniendo los datos

---

[54] Rico Carrillo, M., (2013). *Los desafíos del derecho penal frente a los delitos informáticos y otras conductas fraudulentas en los medios de pago electrónicos.* Ius: Revista Del Instituto De Ciencias Jurídicas De Puebla, nº 31, pp. 207-222.

[55] Artículo 399 *bis* CP: *1. El que altere, copie, reproduzca o de cualquier otro modo falsifique tarjetas de crédito o débito o cheques de viaje, será castigado con la pena de prisión de cuatro a ocho años. Se impondrá la pena en su mitad superior cuando los efectos falsificados afecten a una generalidad de personas o cuando los hechos se cometan en el marco de una organización criminal dedicada a estas actividades.*
*Cuando de acuerdo con lo establecido en el artículo 31 bis una persona jurídica sea responsable de los anteriores delitos, se le impondrá la pena de multa de dos a cinco años.*
*Atendidas las reglas establecidas en el artículo 66 bis, los jueces y tribunales podrán asimismo imponer las penas recogidas en las letras b) a g) del apartado 7 del artículo 33.*
*2. La tenencia de tarjetas de crédito o débito o cheques de viaje falsificados destinados a la distribución o tráfico será castigada con la pena señalada a la falsificación.*
*3. El que sin haber intervenido en la falsificación usare, en perjuicio de otro y a sabiendas de la falsedad, tarjetas de crédito o débito o cheques de viaje falsificados será castigado con la pena de prisión de dos a cinco años.*

de la tarjeta original por medio de un ataque informático. La falsificación sin clonación es más habitual en el comercio electrónico puesto que se ejecuta mediante ataques informáticos de robo de información de las tarjetas de pago. Ambas figuras, al ser similares, se enmarcan en el artículo 399 *bis* del Código Penal antes citado.

Por último, hay que hacer referencia a los supuestos de estafa de tarjetas bancarias. En los casos de estafa no se realiza una captación o uso indebido de los datos de las tarjetas sino que, se provoca un engaño en el sujeto estafado para que este realice, de manera voluntaria, una disposición de dinero a favor del estafador. Las estafas a través del comercio electrónico pueden suscitar problemas en torno a la tipificación del delito puesto que, en muchos de los supuestos, puede faltar alguno de los elementos que configuran la estafa (engaño bastante, error y disposición patrimonial), complicando de esta forma la configuración de las conductas como delitos de estafa. Este problema aparece principalmente por la falta del elemento del engaño pues la jurisprudencia[56], en distintos casos, ha apelado a la falta de diligencia de los compradores al no realizar las suficientes comprobaciones de identidad o legalidad del sitio *web* o comercio electrónico donde estaban realizando la compra. Con la reforma del Código Penal de 2010, se introduce en el artículo 248 un apartado segundo[57], que recoge este tipo de estafas para darles un tratamiento autónomo e independiente de las estafas propias. Dentro del apartado segundo se pueden diferenciar las estafas llevadas a cabo por medio de algún tipo de manipulación informática, las realizadas mediante la fabricación de programas informáticos destinados a la comisión de estafas y las que se producen por el uso indebido de tarjetas en perjuicio de su titular o de un tercero.

Sin embargo, en la actualidad, han aparecido numerosas variaciones y nuevas técnicas para ejecutar estas conductas tales como el *phishing*, *código malicioso*, *pharming*, *vishing*, *spoofing*, *scam*, *spam*, *smishing*, etc. En los siguientes epígrafes se explicarán algunas de las conductas nombradas que se encuentran relacionadas de forma más directa

[56] Rico Carrillo, M., (2013). *Los desafíos del derecho penal frente a los delitos informáticos y otras conductas fraudulentas en los medios de pago electrónicos.* Ius: Revista Del Instituto De Ciencias Jurídicas De Puebla, nº 31, pp. 207-222.

[57] Artículo 248.2 CP: *También se consideran reos de estafa:*
*a) Los que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consigan una transferencia no consentida de cualquier activo patrimonial en perjuicio de otro.*
*b) Los que fabricaren, introdujeren, poseyeren o facilitaren programas informáticos específicamente destinados a la comisión de las estafas previstas en este artículo.*
*c) Los que utilizando tarjetas de crédito o débito, o cheques de viaje, o los datos obrantes en cualquiera de ellos, realicen operaciones de cualquier clase en perjuicio de su titular o de un tercero.*

con el pago con tarjeta y que suponen la captación y el uso indebido de datos, mediante la copia o la obtención de datos personales y bancarios del titular de la tarjeta, los códigos de la tarjeta, claves de acceso, etc.

### 4.1 *Phishing*.

El *'phishing'* procede de las palabras en inglés 'pescar y cosechar'[58]. Se caracteriza por el engaño a los usuarios de las tarjetas bancarias con el fin de obtener sus datos confidenciales, como son los datos personales o las claves de acceso a la banca *online*. El sujeto estafador o *'phisher'*, lleva a cabo el engaño a través del envío de múltiples mensajes de texto mediante correos electrónicos que simulan la procedencia de la *web* de la entidad bancaria. En estos mensajes se comunica a los clientes que tienen que confirmar cierta información vinculada a su cuenta bancaria, como pueden ser alertas de seguridad de la cuenta, avisos de cancelación de las cuentas si no se realizan las actualizaciones correspondientes, etc. Una vez que el sujeto abre el mensaje y pulsa sobre el *link*, es derivado a una página *web* falsa donde ingresa su información personal con el total desconocimiento de la falsedad del sitio *web* y sin ser consciente de que la información va a ser enviada al estafador que, posteriormente, la usará para la realización de transferencias a su favor, hacer pagos, etc.[59]

Mediante esta técnica se crea una falsa apariencia de entidad bancaria como consecuencia de las características del mensaje, en el que aparece el logotipo de la entidad bancaria y una serie de signos distintivos que provocan en el sujeto un engaño bastante para perpetrar la estafa.

Podemos encontrarnos hasta con cinco variaciones de *phishing*:[60]

[58] Egocheaga Cabello, J.E., (2016). *Reclamaciones en materia de Internet y redes sociales.* Reclamaciones en materia de consumo, pp. 279-308.
[59] Domingos Sanca, F. (2013). *Comercio electrónico y pago mediante tarjeta de crédito en el ordenamiento jurídico español: una propuesta para su implementación en el ordenamiento jurídico de Guinea-Bissau.* Universidad Carlos III, Madrid.
[60] Asociación de Usuarios de Bancos, Cajas y Seguros de España (ADICAE). *Catálogo técnico europeo contra el fraude,* p. 66.

1. *Phishing* engañoso.

Es el tipo de *phishing* original, realizado por medios de mensajería instantánea y correo electrónico.

2. *Phishing* basado en *software* malicioso.

La clave que diferencia a este tipo de *phishing* con el resto es la ejecución de un *software* malicioso en el ordenador del sujeto estafado.

3. *Phishing* mediante introducción de contenidos.

Mediante esta modalidad se introduce un *software* malicioso en un sitio *web* legítimo con el fin de redirigir a los visitantes a otra página, instalar *malware* en el ordenador de la víctima, etc.

4. *Phishing* mediante la técnica del intercambio.

Consiste en el posicionamiento del *phisher* entre el ordenador de la víctima y el servidor *web* legítimo, accediendo de esta manera a la información transferida desde el ordenador del usuario al servidor *web*, sin que estos sean conscientes del ataque.

5. *Phishing* de motor de búsqueda.

Esta modalidad se lleva a cabo mediante la creación de páginas *web* para la venta de productos o servicios que cuentan con un precio bajo y atractivo para el consumidor. Una vez creada la página, los estafadores esperan a que las personas la visiten para la compra de los bienes o servicios y de este modo, obtener la información confidencial de los clientes o recibir directamente las transferencias de dinero efectuadas por los compradores.

### 4.2 *Pharming*.

El término *'pharming'* proviene de la palabra 'granja' en inglés (*pharm*) y consiste en un proceso en el que un *hacker* consigue las claves de acceso de un usuario aprovechando las vulnerabilidades que pueda presentar el servidor DNS[61] de un banco o del ordenador del usuario, pudiendo a través de esas vulnerabilidades redirigir un nombre de dominio a otra página distinta. El usuario al teclear en un ordenador el orden de dominio del banco será redirigido a otra página distinta, controlada por el *hacker* que obtendrá toda la información confidencial del sujeto.[62]

El *pharming* suele ser frecuente en aquellos ordenadores que se encuentran infectados por algún tipo de *software* malicioso, que es lo que permite a los *hackers* entrar en los ordenadores de los individuos.

### 4.3 Código Malicioso.

Es un método consistente en el uso de códigos maliciosos especializados en el robo de información. Aprovechando los puntos débiles de la seguridad en *Internet*, se instalan códigos maliciosos para que los usuarios realicen acciones que hagan que el código se instale y puedan acceder a sus ordenadores.[63]

Los códigos maliciosos son cada vez más frecuentes en la red, superando incluso a uno de los métodos más famosos como es el *phishing*. Son ataques más complejos, con una mayor dificultad técnica, y difíciles de prevenir, de identificar y de combatir.[64]

Algunos de los códigos maliciosos más destacables son: los troyanos, *dialers* (marcadores telefónicos), *keyloggers* (registradores de pulsaciones de teclado), virus, gusanos, *rootkits*, *exploits* y macros.

---

[61] '*Domain Name System*' o sistema de nombre de dominio, es un servicio que habilita un enlace entre nombres de dominio y direcciones IP con la que están asociados.
[62] Egocheaga Cabello, J.E., (2016). *Reclamaciones en materia de Internet y redes sociales.* Reclamaciones en materia de consumo, pp. 279-308.
[63] Domingos Sanca, F. (2013). *Comercio electrónico y pago mediante tarjeta de crédito en el ordenamiento jurídico español: una propuesta para su implementación en el ordenamiento jurídico de Guinea-Bissau*. Universidad Carlos III, Madrid.
[64] Asociación de Usuarios de Bancos, Cajas y Seguros de España (ADICAE). *Catálogo técnico europeo contra el fraude,* p. 57.

## 5. CONCLUSIONES.

*La primera conclusión* que me gustaría destacar es la relevancia que tiene la protección de datos de carácter personal, habida cuenta de la continua exposición a la que se encuentran sometidos los ciudadanos, y su influencia en la intimidad, la dignidad y el honor. Hoy, tras más de un siglo desde su origen en Estados Unidos con el '*Right to Privacy*', la protección de datos se posiciona entre uno de los derechos más presentes en el día a día de los sujetos, con necesidades cada vez mayores y en continua actualización.

*La segunda conclusión*, una vez analizadas las diferentes legislaciones relativas a este derecho es que, la LGPD y el RGPD se sitúan como dos marcos de referencia sobre los que hay que trabajar para la progresiva adaptación a los nuevos requerimientos de protección. Si bien estas normas dejan algunos interrogantes y/o lagunas jurídicas que la jurisprudencia tanto nacional como supranacional deberán ir cumplimentando.

*La tercera conclusión*, hace mención al comercio electrónico como nueva forma de comercio que ha llegado para quedarse, y con él, nuevos y numerosos sistemas de pago *online*. Parece obvio que las transacciones electrónicas se están imponiendo cada vez más (incrementándose con motivo de la pandemia Covid-19). Son muchos los retos y desafíos que ofrecen y que se han intentado resumir en el presente trabajo.

*La cuarta conclusión*, tiene a las tarjetas bancarias como protagonistas de la misma para destacar, que tal y como se ha reflejado, su uso puede dar lugar a brechas en la seguridad de nuestros datos y por lo tanto, tener como resultado una vulneración del derecho fundamental a la protección de datos. El sistema de pago mediante tarjetas bancarias ha sido uno de los ejes centrales de la investigación. Es el sistema más empleado en las transacciones de comercio electrónico, fácil de utilizar pero complejo por la sensibilidad de los datos que se intercambian.

*Finalmente*, es preciso hacer hincapié en el papel de las entidades bancarias y los comercios *online* como uno de los encargados de incorporar las medidas necesarias en sus servicios y páginas *webs* para ofrecer seguridad en las transacciones. En esta misma línea, la figura de los proveedores de servicios de pago tiene también un papel importante en la lucha contra los fraudes en los instrumentos de pago puesto que, tienen el poder de dar una respuesta inmediata en el análisis de los delitos y fraudes que pueden acontecer en sus servidores.

De cara al futuro, entiendo que los operadores jurídicos tienen el reto de hacer que la protección de datos de carácter personal vaya de la mano con todos los cambios y las innovaciones que traigan consigo las nuevas tecnologías, para velar siempre por los derechos de los ciudadanos que debe ser el objetivo de los mismos.

## 6. BIBLIOGRAFÍA.


- Aliño Sehwerert, J., (2018). *La protección del consumidor digital: los datos personales en el comercio electrónico*. Revista Jurídica sobre Consumidores y Usuarios., 3, pp.97-115.

- Bellovin, S.M, Hutchins, R.M, Jebara, T, Zimmeck, S. (2013). *"When enough is enough: Location Tracking, Mosaic Theory, and Machine Learning", New York University Journal of Law & Liberty.*

- Cazurro Barahona, V. (2020). *Antecedentes y fundamentos del Derecho a la protección de datos*. pp. 19-46. Barcelona: J. M. Bosch.

- Domingos Sanca, F. (2013). *Comercio electrónico y pago mediante tarjeta de crédito en el ordenamiento jurídico español: una propuesta para su implementación en el ordenamiento jurídico de Guinea-Bissau.* Universidad Carlos III, Madrid.

- Egocheaga Cabello, J.E., (2016). *Reclamaciones en materia de Internet y redes sociales.* Reclamaciones en materia de consumo, pp. 279-308.

- Escobar, E. M. (2000). *El comercio electrónico: perspectiva presente y futura en España*. Madrid: Fundación Retevisión.

- Madrid Conesa, F. (1984). *Derecho a la intimidad, informática y estado de derecho.* p. 45. Valencia: Universidad de Valencia.

- Martín, P., (2018). *Teletrabajo Y Comercio Electrónico*. Madrid: Ministerio de Educación, Cultura y Deporte.

- Rico Carrillo, M., (2013). *Los desafíos del derecho penal frente a los delitos informáticos y otras conductas fraudulentas en los medios de pago electrónicos.* Ius: Revista Del Instituto De Ciencias Jurídicas De Puebla, nº 31, pp. 207-222.

- Urbano Mateos, S., (2016). *Qué es y cómo funciona la pasarela de pago en ecommerce*. Blog: *Actualidad E-commerce,*

## 7. LEGISLACIÓN.

- Carta de los Derechos Fundamentales UE.

- Código Penal.

- Constitución Española.

- Directiva (UE) 2015/2366 del Parlamento Europeo y del Consejo, de 25 de noviembre de 2015 sobre servicios de pago en el mercado interior.

- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

- Ley 16/2009, de 13 de noviembre, de Servicios de Pago.

- Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico.

- Real Decreto-ley 19/2018, de 23 de noviembre, de Servicios de Pago y otras Medidas Urgentes en Materia Financiera

- Recomendación 87/589/CEE de la Comisión, de 8 de diciembre de 1987, sobre el Código Europeo de Buena Conducta.

- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016.

## 8. JURISPRUDENCIA.

- Sentencia del Tribunal Constitucional 292/2000 de 30 de noviembre.

## 9. WEBGRAFÍA Y SIMILARES.


- Agencia Española de Protección de Datos: *Compra segura en Internet. Guía prática.*

  Online: https://www.aepd.es/sites/default/files/2019-09/guia-compra-segura-digital-web.pdf

- Agencia española de protección de datos.

  Online: https://datos.redomic.com/Archivos/GuiasUtiles/G33.pdf

- Asociación de Usuarios de Bancos, Cajas y Seguros de España (ADICAE). *Catálogo técnico europeo contra el fraude.*

- Comisión Europea.

  Online: https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_es#:~:text=Los%20datos%20personales%20son%20cualquier,constituyen%20datos%20de%20car%C3%A1cter%20personal.

- Comisión Europea. Protección de datos.

  Online: https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_es

- Comisión Nacional de los Mercados y la Competencia.

  Online: http://data.cnmc.es/datagraph/

- Diccionario panhispánico del español jurídico.

  Online: https://dpej.rae.es/lema/derecho-al-honor

- Eleconomista.es. (2020). *Entidad Emisora: Qué Es - Diccionario De Economía*.

  Online: https://www.eleconomista.es/diccionario-de-economia/entidad-emisora

- El Economista: *La tendencia en el comercio electrónico la marcarán los 'marketplaces' en 2021* (30 noviembre 2020).

  Online: https://www.eleconomista.es/tecnologia/noticias/10916924/11/20/En-2021-los-mercados-online-marcaran-tendencia-en-el-comercio-electronico-.html

- Observatorio Nacional de las Telecomunicaciones y de la Sociedad de la Información (ONTSI), *El comercio electrónico B2C en España 2019 (Edición 2020).*
- Organización Mundial del Comercio (OMC).

- Real Academia Española.