CUNEF
COLEGIO UNIVERSITARIO DE
ESTUDIOS FINANCIEROS

Máster Universitario de Acceso a la Profesión de Abogado

2018 – 2020

Trabajo de Fin de Máster

Ciberseguridad y protección de datos en el ámbito de las transacciones comerciales electrónicas

---

Alumna: D.ª Elisa Castejón López de Ayala

Tutor: Prof. Dr. D. Daniel Berzosa López

Madrid, febrero de 2020

ÍNDICE

1. ABREVIATURAS

- **AELC:** Asociación de Libre Comercio.
- **ARPANET:** Red de la Agencia de Proyectos de Investigación Avanzada.
- **ART:** Artículo.
- **CDFUE:** Carta de los Derechos Fundamentales de la Unión Europea
- **CC:** Código Civil.
- **CE:** Constitución Española 1978.
- **CEE:** Comunidad Económica Europea.
- **CMSI:** Cumbre Mundial sobre la Sociedad de la Información.
- **CNU:** Convención de Naciones Unidas.
- **DARPA:** Agencia de Proyectos de Investigación Avanzados de Defensa
- **DOD:** Departamento de Defensa de Estados Unidos.
- **DOUE:** Diario Oficial de la Unión Europea.
- **DIRECTIVA 2000/31/CE:** Directiva 2000/31/CE del Parlamento Europeo y del Consejo de 8 de junio de 2000 relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior.
- **EEE:** Espacio Económico Europeo.
- **EFT:** Transferencias Electrónicas.
- **IEEE:** Instituto Español de Estudios Estratégicos.
- **LOPD:** Ley Orgánica 3/2018 de Protección de Datos Personales y garantía de los derechos digitales.
- **OMC:** Organización Mundial del Comercio.
- **RGPD:** Reglamento General de Protección de Datos.
- **TFUE:** Tratado de Funcionamiento de la Unión Europea.
- **TICs:** Tecnologías de la Información y la Comunicación.
- **UE:** Unión Europea.
- **UIT:** Unión Internacional de Telecomunicaciones.
- **WWW:** World Wide Web.

2. INTRODUCCIÓN

El siglo XXI ha abierto las puertas de la era tecnológica y con ello el nacimiento de un nuevo tipo delictivo, el ciberataque, cuyo principal objetivo son los datos de carácter personal contenidos en las bases de datos que se encuentran en la red, almacenando y custodiando miles de datos de este tipo.

Esta tecnología informática ha contribuido al crecimiento de la economía por medio de las transacciones comerciales electrónicas. Gracias a esta evolución, el comercio tradicional ha traspasado fronteras evolucionando hacia un mercado *on-line* y digitalizado en el que la compra y venta de productos tiene un alcance mundial.

De este modo, el presente trabajo analiza la evolución de las transacciones comerciales electrónicas y con ello, todo lo que acarrea la existencia de una red informática que permite realizar este tipo de transacciones. Exponiendo las ventajas que supone esta evolución hacia el comercio electrónico, pero sin olvidar también las desventajas de este.

Ahondando más en el fondo del asunto y así comprender mejor el mecanismo de funcionamiento de las transacciones comerciales electrónicas en relación con los datos de carácter personal que se generan y almacenan en estas operaciones, se hace un análisis de la Directiva 2000/31/CE del Parlamento Europeo y del Consejo de 8 de junio de 2000 relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior. En esta Directiva se tratan cuestiones tales como la regulación del funcionamiento del mercado interior garantizando la libre circulación de información dentro de la UE, o las obligaciones legales que tiene toda entidad que preste sus servicios vía Internet, y por medio de la que se soliciten datos de carácter personal.

Por ello, los datos de carácter personal almacenados en la red han de ser tratados con la mayor diligencia posible, ya que se trata de información confidencial que se encuentra expuesta con facilidad a cualquier ataque por tratarse de la red el lugar de almacenamiento de estos datos.

De este modo, los ataques que sufren los usuarios de la red se encuentran tipificados como delitos informáticos y se conocen con el nombre de “ataques cibernéticos”. Sin embargo, gracias al Reglamento General de Protección de Datos (Reglamento 2016/679) estos datos personales cuentan con una mayor protección. Además, el derecho al honor y a la intimidad personal y familiar limitando el uso de la informática, ha sido reconocido en más de una ocasión como un derecho fundamental. Así lo reconocen la Carta de los Derechos Fundamentales de la Unión Europea, el Tratado de Funcionamiento de la Unión Europea y la Constitución Española.

Desde una perspectiva más práctica de los conceptos expuestos anteriormente, se plantea y analiza el caso del robo de datos a Uber (2016) en el que un grupo de hackers lleva a cabo el robo de millones de datos de carácter personal de los usuarios de este servicio, viendo así afectada su privacidad e intimidad personal y por consiguiente violando su derecho fundamental al honor y a la intimidad personal. Además, este caso tiene la aplicación del RGPD de un lado en lo que al robo de datos se refiere, y de otro, en relación con el comportamiento de la compañía al descubrir el hackeo de los datos, ya que su principal obligación es informar a la autoridad de control competente y a los titulares de esos datos.

3. TRANSACCIONES COMERCIALES ELECTRÓNICAS

3.1. MARCO CONCEPTUAL

La definición que utiliza Del Peso (2003) para abarcar el concepto de *comercio* desde una perspectiva on-line es *"*negociación que se hace comprando y vendiendo o permutando géneros, mercancías o valores para aumentar el caudal" *(Real Academia de la Lengua 1992: 365).*

No obstante, antes de entrar a definir lo que es una transacción comercial electrónica debemos entender el concepto de transacción en su esencia más pura.

Podría entenderse como un acuerdo al uso entre dos o más partes, en el que el objeto principal es el intercambio de bienes o derechos con una contraprestación normalmente económica.

Esta definición podemos asimilarla a lo que comúnmente se conoce como *"compra venta"*, transacción comercial más común en el Derecho Civil Español. El Código Civil lo regula en su artículo 1445 así: «Por el contrato de compra y venta uno de los contratantes se obliga a entregar una cosa determinada y el otro a pagar por ella un precio cierto, en dinero o signo que lo represente».

En el ámbito internacional, se define más como transacción mercantil que comercial. Así pues, la Convención de Naciones Unidas sobre las inmunidades jurisdiccionales de los Estados y de sus bienes[1], con fecha 16 de diciembre de 2004, establece en el art. 2.1.c la siguiente definición de *transacción comercial*:

> *"i) todo contrato o transacción mercantil de compraventa de bienes o prestación de servicios;*
>
> *ii) todo contrato de préstamo u otra transacción de carácter financiero, incluida cualquier obligación de garantía o de indemnización concerniente a ese préstamo o a esa transacción;*

[1] La Convención de Naciones Unidas sobre las inmunidades jurisdiccionales de los Estados y de sus bienes surge con la idea de fortalecer el derecho y la seguridad jurídica, en concreto en las relaciones de los Estados con las personas físicas y/o jurídicas, y contribuir al desarrollo y codificación del derecho internacional y a armonizar la práctica en este ámbito.

iii) cualquier otro contrato o transacción de naturaleza mercantil, industrial o de arrendamiento de obra o de servicios, con exclusión de los contratos individuales de trabajo." (CNU 2004: art. 2.1.c)

No obstante, las transacciones a las que se harán referencia en este trabajo son las conocidas como *transacciones comerciales electrónicas*, basadas en los mecanismos informáticos y telemáticos actuales.

Este avance tecnológico que nos permite hablar de comercio electrónico (o transacción comercial) recibe el nombre de *sociedad de la información*. Este concepto supone la evolución de las relaciones entre Estados, personas y entidades por medio del uso de las tecnologías de la información y la comunicación[2] (TIC) que nos permiten transmitir y administrar cualquier tipo de información. Tal es la importancia de la sociedad de la información que en 2003 tuvo lugar la primera Cumbre Mundial sobre la Sociedad de la Información[3].

3.2. TRANSACCIONES COMERCIALES ELECTRÓNICAS

Debido al gran avance tecnológico sufrido en los últimos años, es necesario que la definición de transacción comercial vaya más allá de la realidad física entre dos o más partes, extendiéndose de este modo al ámbito cibernético, en el que cada vez más, se llevan a cabo este tipo de transacciones comerciales.

Así pues, por transacción comercial electrónica se entiende cualquier transacción de carácter monetario realizada entre consumidores, usuarios o empresas a través de la red, es decir, Internet, base fundamental del concepto de transacción comercial electrónica.

---

[2] Las TICs son un conjunto de sistemas necesarios para administrar la información y, especialmente, los ordenadores y programas necesarios para convertirla, almacenarla, administrarla, transmitirla y encontrarla *(Fueyo, D. Programar para el aula en la etapa de educación primaria LOE, Lulu, Oviedo: 2010: 81).*

[3] La Cumbre Mundial sobre la Sociedad de la Información (CMSI) fue un evento internacional organizado por la Unión Internacional de Telecomunicaciones (UIT) centrado en los aspectos sociales de la Sociedad de la Información. El objetivo de esta cumbre era eliminar la brecha digital existente en el mundo, sobre todo en las Telecomunicaciones e Internet, y preparar planes de acción y políticas.

La Organización Mundial del Comercio[4] define el comercio electrónico como "la producción, distribución, comercialización, venta y entrega de bienes y servicios por medios electrónicos. Es decir, es el conjunto de transacciones comerciales y financieras realizadas por medio electrónicos, incluyendo texto, sonido e imagen; vendría a ser un sistema global que utilizan redes informáticas y en particular Internet permite crear un mercado electrónico"[5].

Por medio de esta herramienta tecnológica se genera un gran tráfico de información basado en datos, de ahí la necesidad de la creación de normativa que regule estas transacciones, tanto a nivel de regulación y funcionamiento de este comercio electrónico por medio de la Directiva 2000/31/CE del Parlamento Europeo y del Consejo de 8 de junio de 2000 relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior, como en el ámbito de los datos, por medio del 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, texto pertinente a efectos del Espacio Económico Europeo[6] que analizaremos posteriormente.

Hecha esta aclaración, es importante destacar la existencia de varios tipos de comercio electrónico. De un lado, según Del Peso (2003) en su libro *Servicios de la sociedad de la información*, la existencia de varios tipos de comercio electrónico se debe al objeto perseguido, diferenciando así las siguientes categorías:

- Por cómo se perfecciona el contrato.

[4] La Organización Mundial del Comercio es una organización internacional fundada el 1 de enero de 1995 en Suiza. Se encarga de las normas que rigen el comercio entre los países. Tiene como objetivo ayudar a los productores de bienes y servicios, los exportadores y los importadores a llevar adelante sus actividades.

[5] Esta definición de comercio que hace la Organización Mundial del Comercio procede del apartado 1.3 del Programa de trabajo adoptado por el Consejo General el 25 de septiembre de 1998. [en línea] disponible en <https://www.wto.org/spanish/tratop_s/ecom_s/wkprog_s.htm> [13 noviembre 2019]

[6] El Espacio Económico Europeo fue creado en 1994 por los países miembros de la Unión Europea y de la Asociación de Libre Comercio (AELC) excepto Suiza, permitiendo a los Estados que no eran miembros de la Unión participar en el mercado interior de la misma sin necesidad de adherirse a ella.

- Por el medio de pago.
- Por el tipo de red.
- Por el ámbito de aplicación.
- Por el resultado.
- Según las partes que intervienen.

En cuanto a la perfección del contrato, éste puede considerarse *comercio electrónico perfecto* o *comercio electrónico imperfecto.* En el primero todas las fases de la transacción se realizan de manera electrónica, mientras que en el segundo el pago y la entrega se realizan conforme al método tradicional de compraventa.

La distinción hecha en función del medio de pago distingue de un lado el pago dentro de la red, por medio de dinero electrónico, tarjetas de débito, crédito o empresa y de otro, el pago fuera de la red, en metálico, reembolso postal, transferencia bancaria o tarjeta de débito, crédito o empresa.

Por el tipo de red hay que distinguir las redes externas, como es el caso de Internet, y las redes internas, como las redes propias o las redes públicas protegidas.

En lo que respecta al ámbito de aplicación, bien es cierto que cada vez nos encontramos en un mundo más globalizado, pero no hay que dejar a un lado esta categoría ya que supone un aspecto fundamental en cuanto a la legislación y normas de aplicación. Por tanto, podrá ser nacional, comunitario e internacional en función de dónde operan las partes contratantes.

Por el resultado se distingue entre válido, cuando no existen causas que lo invaden, y no válido, cuando el contrato no cuenta con los requisitos requeridos para hacerse efectivo *(Del Peso 2003: 21-23).*

Finalmente, el método más utilizado para hacer una distinción de los tipos de comercio electrónico es según quiénes sean las partes en la transacción efectuada nos encontramos con tres tipos: cuando las dos partes son empresas *Business to Business* (B2B), cuando las partes son empresa y consumidor *Business to Consumer* (B2C) y cuando las partes son consumidores *Consumer to Consumer* (C2C) *(Alonso 2004:15).*

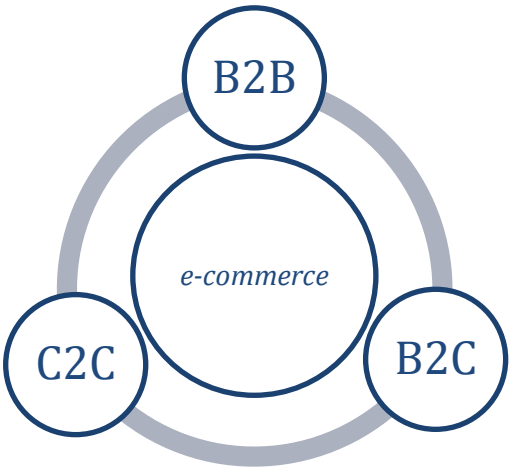


Figura 1. E-commerce y sus tipos
Fuente propia

En el comercio electrónico de B2B se llevan a cabo transacciones online en las que las dos partes contratantes son empresas. Concretamente entre una empresa y un proveedor, banca, abogados, Estado, etc. Permite que por medio de Internet se agilicen los intercambios de bienes y servicios.

Este tipo de comercio electrónico tiene su origen en el Intercambio Electrónico de Datos (EDI), servicio basado en el intercambio de información, en concreto documentos estandarizados entre empresas que se encuentran relacionadas por el comercio. Sobre todo, se hace en relación con facturas, albaranes, contabilidad, y demás cuestiones administrativas, lo que supone además de una agilización y economización del tiempo.

El comercio electrónico B2C es aquel en el que una empresa (*business*) vende un producto a un tercero, que en este caso es el consumidor final (*consumer*). Es la práctica más común además de la más conocida. Supone todo el proceso de compra venta, es decir, desde la publicidad de los productos en la red, hasta la venta de estos por medio de cobros seguros para atraer la confianza de sus clientes que son los consumidores a los que se refiere la letra C de B2C. En este tipo de transacción electrónica al cliente se le denomina *'ciberconsumidor'* y es el que hace que el comercio del empresario se oriente de una manera u otra.

En el comercio electrónico de C2C el intercambio de bienes y servicios se lleva a cabo de ambos lados entre particulares. Es la práctica menos común, aunque cada vez son más los usuarios de la red los que lo usan.

Por tanto, podemos entender el comercio electrónico como toda aquella actividad que supone una contraprestación económica y se realice a través de una red de Internet.

3.3. EVOLUCIÓN HISTÓRICA DEL COMERCIO ELECTRÓNICO

El comercio electrónico, también conocido como *e-commerce*[7] ha ido evolucionando a lo largo de la historia de la mano del que ha sido su pilar fundamental, Internet. En sus inicios no era más que una serie de aplicaciones destinadas a la transferencia de fondos monetarios, pero con los grandes avances que se han ido produciendo en el mundo electrónico a lo largo de las últimas décadas, ha tomado una posición ventajosa frente al comercio tradicional y sus prácticas cotidianas.

Internet nace en 1969 cuando la Agencia de Proyectos de Investigación Avanzados de Defensa (por sus siglas en inglés, DARPA)[8] decide crear una red de computadores que denominó ARPANET. Fue creada por el Departamento de Defensa de Estados Unidos (DOD) para que la comunicación entre las diferentes instituciones académicas y estatales fuesen más fluidas.

Sin embargo, no es hasta 1991 cuando surge el *e-commerce*. Este método de transacción comercial surge con la noción de “vender y comprar” cuando Internet hace posible la comercialización online.

La década de los 70 generó una gran revolución en el ámbito de las transacciones comerciales electrónicas. En los inicios de esta década con la creación de Internet ya vigente, se llevan a cabo las primeras transferencias electrónicas (EFT) entre entidades bancarias dando lugar a una revolución en los mercados financieros

[7] *E-commerce* es una nomenclatura de origen inglesa procedente del término electronic commerce.
[8] *Defense Advanced Research Projects Agency*, es una agencia del Departamento de Defensa de Estados Unidos responsable del desarrollo de nuevas tecnologías para uso militar.

y permitiendo a los usuarios el intercambio de información. A finales de esta década y a principios de los años 80, pese a que el correo electrónico fue creado dos décadas antes, se extiende en compañías, así como el Intercambio Electrónico de Documentos (EDI). Este último elemento supuso una reducción en el coste de las materias primas.

A finales del siglo XX, en la década de los 90, Tim Berners-Lee[9] crea la World Wide Web (en adelante WWW). Esta acepción engloba un mecanismo electrónico cuya finalidad consiste en la distribución de soportes documentales o multimedia que se encuentran interconectados entre sí y que son accesibles a través de Internet. Este término engloba lo que se conoce más comúnmente como páginas web. De ahí que la mayoría de las direcciones web contengan el prefijo “www”.

Así fue la primera red creada por la Word Wide Web:

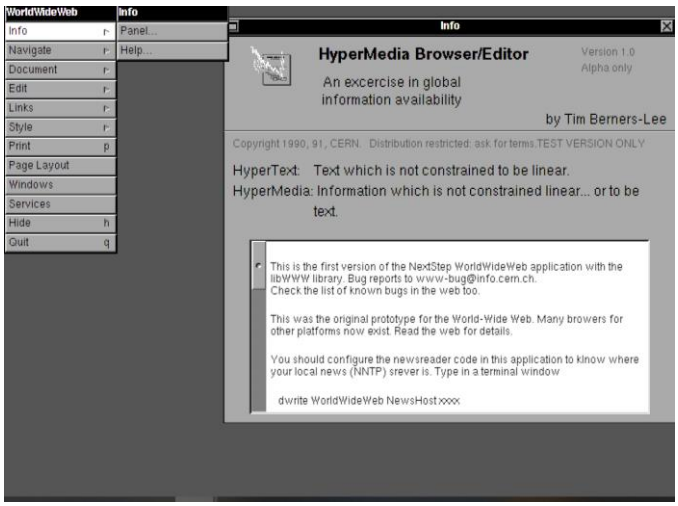


Figura 2. Primera web creada por Word Wide Web.
Fuente: https://worldwideweb.cern.ch/browser/

Este sistema informático es la mayor red mundial de contenido, por encima de Google. Esta afirmación está además refrendada en la indexación[10] que se origina en

[9] Tim Berners-Lee (Londres, Reino Unido, 8 de junio de 1955) científico de la computación británica, conocido por ser el padre de la World Wide Web.
[10] Indexación: mecanismo que incluye en el índice de internet el contenido de un sitio web. En ocasiones se utiliza lo que se conoce como índice de back-of-the-book, mientras que los motores de búsqueda suelen utilizar palabras clave y metadatos (metaetiquetas) para proporcionar un vocabulario más útil para Internet o la búsqueda en el sitio.

la misma. Así en la siguiente gráfica se puede observar el análisis hecho por Google de la indexación en WWW en los últimos cuatro meses del año 2019.

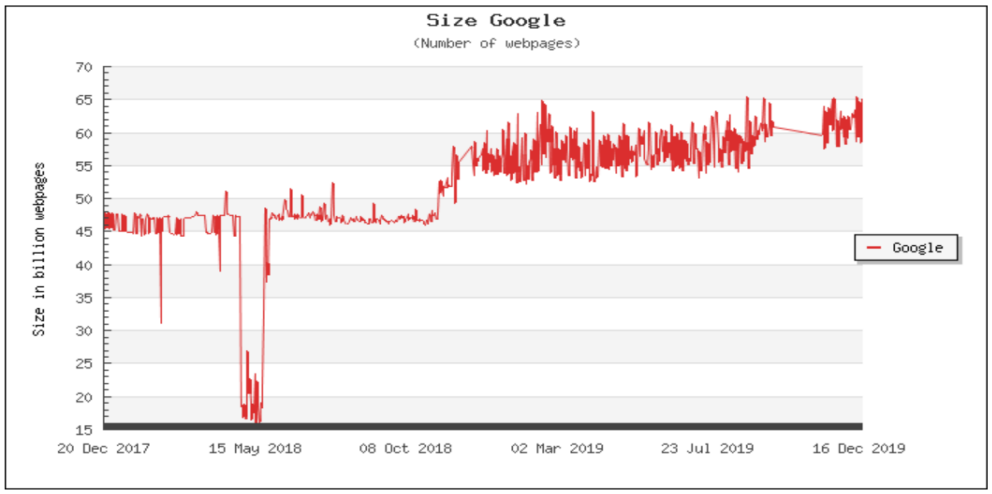


Figura 3. Gráfica de la indexación en WWW en los últimos 4 meses de 2019
Fuente: página web WWW: https://www.worldwidewebsize.com

3.4. VENTAJAS E INCONVENIENTES DEL COMERCIO ELECTRÓNICO

3.4.1. Ventajas

El comercio electrónico o *e-commerce*, es una práctica comercial que ha evolucionado de la mano de Internet y que goza de un gran número de ventajas.

En el ámbito empresarial, el comercio electrónico ha supuesto un aumento considerable de ingresos para todos aquellos que han sabido hacer uso de este. En sus inicios, era un método complementario a la venta física, pero con el paso de los años y los grandes avances tecnológicos que se están experimentando en esta última década, en ocasiones este método transaccional es el elegido única y exclusivamente para llevar a cabo actividades económicas, ya que puede llegar a suponer un menor coste respecto al comercio tradicional.

Esta es la primera ventaja que destacar; la agilidad, facilidad y economicidad que trae consigo el desarrollo de una actividad económica cibernética o, mejor dicho, *e-commerce.*

De otro lado, supone una ventaja para las pequeñas y medianas empresas ya que a través de Internet es más difícil discernir entre el volumen de negocio de las empresas, que en ocasiones condiciona a los compradores a la hora de efectuar una compra por considerar menos fiable una empresa de menor tamaño.

Además de esto, Internet hace posible la venta de productos todos los días del año, con independencia de los horarios de apertura y cierre o los días feriados. A esto hay que sumarle la facilidad que proporciona a los clientes en lo que al desplazamiento se refiere, ya que pueden efectuar la compra de los productos desde cualquier lugar siempre que tengan conexión a la red.

En cuestiones más económicas, como he mencionado anteriormente, supone un menor coste para la empresa, ya que los gastos de personal e instalaciones disminuyen e incluso en ocasiones no existen por tratarse de una empresa 100% online.

No obstante, las ventajas no solo son para el empresario, también el cliente se beneficia de ciertas ventajas como son las siguientes:

En primer lugar, pueden llevar a cabo un análisis más exhaustivo del mercado, comparando al mismo tiempo los precios y productos que ofrecen las empresas competidoras, y así comprar la opción más acorde a su situación económica *(De Miguel 2008: 156).*

Como he mencionado en las ventajas empresariales, el *e-commerce* facilita también a los consumidores la compra de los productos sin tener que desplazarse. Además, hay una mayor facilidad a la hora de adquirir productos que en la tienda física se encuentran agotados o fuera de stock, pero que sin embargo en la tienda online sí hay mayor posibilidad de adquirir estos productos.

3.4.2. Inconvenientes

Al igual que todos los negocios, el *e-commerce* también tiene una serie de desventajas frente al comercio tradicional que llegan a ser comunes para empresas y consumidores, ya que lo que supone una desventaja para los consumidores lo es por

consiguiente para las empresas, pues son los clientes los que hacen que el negocio funcione.

En lo que respecta a las desventajas que sufren las empresas encontramos las siguientes:

En primer lugar, la edad media de las personas que hacen uso de internet es de 35 años, por lo que un gran número de la población queda fuera de este parámetro. Suelen ser personas que optan por la compra física, lo que acarrea una pérdida de ingresos para las empresas cuya facturación online supone la mayor parte de sus ganancias.

Otro de los aspectos de la compra online que contribuye a que el número de ventas sea menor es la fiabilidad en los productos, ya que el hecho de no poder verlos físicamente antes de la compra crea dudas en los clientes y en muchas ocasiones es el detonante para no concluir con la compra del producto. De otro lado, la fiabilidad de la red supone también una gran desventaja, ya que en muchas ocasiones los clientes no encuentran seguros los medios de pago ni la protección de sus datos personales *(De Miguel, 2008: 155).*

Schneider señala también que el desconocimiento de la persona que encarna la figura del vendedor es también un inconveniente para los compradores a la hora de efectuar una compra online.

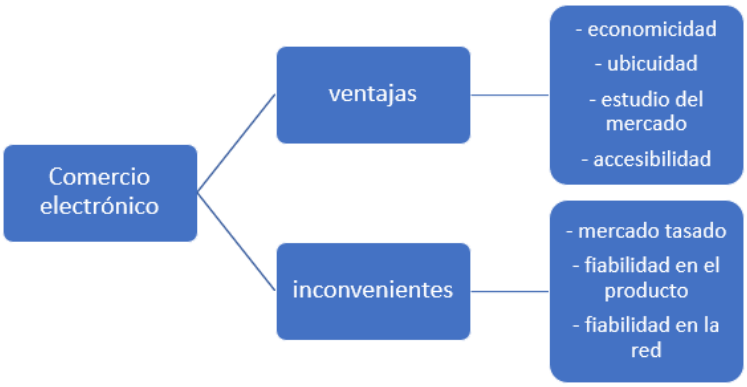


Figura 4. Ventajas y desventajas del comercio electrónico.
Fuente propia.

Pese a estas desventajas, en el caso de empresas que combinan la venta física con la venta online siempre va a resultar una valoración positiva ya que, si no recibe ingresos de un lado, lo hará de otro. Distinto es el caso de aquellas empresas en las que su único punto de venta es online, ya que esto puede excluir a ciertos sectores de la población que por determinadas circunstancias ya sean económicas, culturales e incluso relativas a la edad.

4. REGULACIÓN LEGAL DEL COMERCIO ELECTRÓNICA

4.1. Directiva 2000/31/CE Del Parlamento Europeo y del Consejo de 8 de junio de 2000

El comercio electrónico encuentra su regulación legal en la Directiva 2000/31/CE del Parlamento Europeo y del Consejo de 8 de junio de 2000 relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior (Directiva sobre el comercio electrónico).

Esta directiva ha sido traspuesta al Ordenamiento Jurídico español mediante la *Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico*. No obstante, y debido a que el comercio electrónico abarca un campo tan extenso como todos aquellos lugares donde los usuarios tengan acceso a una red, es decir, más allá de las fronteras de nuestra nación, nos centraremos en analizar la Directiva en cuestión.

En primer lugar, como toda Directiva, esta es una disposición normativa de Derecho comunitario que vincula a todos los Estados de la Unión, como se indica en el art. 24 de la misma.

Su aprobación tuvo lugar en Luxemburgo el 8 de junio de 2000, visto por el Parlamento Europeo y el Consejo de la Unión Europea. Además, hay que distinguir otra fecha; el 17 de julio de 2000, día en el que se publicó y entró en vigor la presente Directiva. Finalmente, en cuanto a la trasposición por parte de los Estados miembros, ésta no podría ser posterior al 17 de enero de 2002 como así viene estipulado en el texto.

En lo que a la estructura se refiere, está dividida en 4 capítulos:

- Capítulo I: Disposiciones Generales
- Capítulo II: Principios
- Capítulo III: Aplicación
- Capítulo IV: Disposiciones finales

Que a su vez se encuentran subdivididos en secciones y artículos del siguiente modo:

El Capítulo I contiene los artículos 1 - 3 titulados:

- Art. 1. Objetivo y ámbito de aplicación
- Art. 2. Definiciones
- Art. 3. Mercado interior

El Capítulo II, regula los artículos 4 - 15 titulados y divididos del siguiente modo:

➢ Sección 1: Régimen de establecimiento y de información

- Art. 4. Principios de no autorización previa
- Art. 5. Información general exigida

➢ Sección 2: Comunicaciones comerciales

- Art. 6. Información exigida
- Art. 7. Comunicación comercial no solicitada
- Art. 8. Profesiones reguladas

➢ Sección 3: Contratos por vía electrónica

- Art. 9. Tratamiento de los contratos por vía electrónica
- Art. 10. Información exigida
- art. 11. Realización de un pedido

➢ Sección 4: Responsabilidad de los prestadores de servicios intermediarios

- Art. 12. Mera transmisión

- Art. 13. Memoria tampón *(Caching)*
- Art. 14. Alojamiento de datos
- Art. 15. Inexistencia de obligación general de supervisión

El Capítulo III titulado de la Aplicación regula los artículos 16 - 20 titulados:

- Art. 16. Códigos de conducta
- Art. 17. Solución extrajudicial de litigios
- Art. 18. Recursos judiciales
- Art. 19. Cooperación
- Art. 20. Sanciones

Por último, el Capítulo IV que regula las Disposiciones finales contiene los artículos 21 - 24:

- Art. 21. Reexamen
- Art. 22. Trasposición
- Art. 23. Entrada en vigor
- Art. 24. Destinatarios

En cuanto al análisis de su contenido, en primera instancia nos encontramos en el art. 1 con el *objetivo y ámbito de aplicación* de la Directiva. En él se pretende regular el funcionamiento del mercado interior, garantizando la libre circulación de información *(Directiva 2000: art. 1.1).* Además, para hacer posible este precepto, se llevará a cabo la aproximación de las disposiciones nacionales aplicables que sean necesarias *(Directiva 2000: art. 1.2).*

El art. 2 titulado *Definiciones* hace una breve descripción de determinados conceptos necesarios para entender esta Directiva. Concretamente, en el apartado a) del mismo remite a consultar la Directiva 98/34/CE, modificada por la Directiva 98/48/CE, concretamente a su art. 1.2.

Por tanto, acudimos a la Directiva 98/34/CE que define los servicios de la sociedad de la información así:

"2) «servicio»: todo servicio de la sociedad de la información, es decir, todo servicio prestado normalmente a cambio de una remuneración, a distancia, por vía electrónica y a petición individual de un destinatario de servicios.

A efectos de la presente definición, se entenderá por:

- *a distancia, un servicio prestado sin que las partes estén presentes simultáneamente;*
- *por vía electrónica, un servicio enviado desde la fuente y recibido por el destinatario mediante equipos electrónicos de tratamiento (incluida la compresión digital) y de almacenamiento de datos y que se transmite, canaliza y recibe enteramente por hilos, radio, medios ópticos o cualquier otro medio electromagnético;*
- *a petición individual de un destinatario de servicios, un servicio prestado mediante transmisión de datos a petición individual. (…)*

La presente Directiva no será aplicable:

- *a los servicios de radiodifusión sonora,*
- *a los servicios de radiodifusión televisiva contemplados en la letra a) del artículo 1 de la Directiva 89/552/CEE."* (Directiva 2000/31/CE, 2000)

De otro lado, en el apartado f) de este mismo artículo se define el concepto de *"comunicación comercial"* como una manera de comunicación que tiene por objeto proporcionar bienes, servicios o la imagen de cualquier corporación de manera directa o indirecta. Además excluye de la definición de comunicaciones comerciales todos aquellos datos que permiten el acceso directo a las actividades que desarrollan las corporaciones mencionadas anteriormente, en concreto el nombre de dominio o la dirección de correo electrónico así como las relativas a bienes, servicios o imagen de la empresa cuando se realiza sin contraprestación económica así como aquellas comunicaciones referentes a bienes, servicios e incluso a la imagen de las empresas concretamente cuando se hace de manera independiente a ellas y sin remuneración *(Directiva 2000/31/CE 2000: art.2).*

En el art. 3 del *Mercado interior* se regula cómo los Estados miembros han de velar por el buen uso de los servicios de la sociedad de la información, para que cumplan las normas del Estado miembro en el que se lleve a cabo *(Directiva 2000/31/CE 2000: art. 3.1).*

El art. 5 regula la *Información general exigida* y lo hace indicando que los Estados miembros han de garantizar que el prestador de servicios permita tanto a destinatarios como a autoridades competentes el acceso a los siguientes datos:

- el nombre de aquella persona o entidad que presta el servicio
- la ubicación/dirección geográfica donde se encuentra el prestador de servicio
- los datos identificativos del prestador de servicios
- nombre del registro en el que se encuentra inscrito el prestador
- los datos de la autorización que supervisa la actividad
- los datos del colegio profesional, el título profesional expedido y el Estado miembro en que se expidió, así como la referencia a las normas profesionales que le son aplicables.
- en caso de una actividad gravada por el IVA,

  el número de identificación a que hace referencia el apartado 1 del artículo 22 de la Sexta Directiva 77/388/CEE del Consejo, de 17 de mayo de 1977, en materia de armonización de las legislaciones de los Estados miembros relativas a los impuestos sobre el volumen de negocios (Directiva 2000/31/CE 2000: art. 5.1).

Una vez analizados los aspectos más teóricos, llegamos al art. 9 titulado Tratamiento de los contratos por vía electrónica, por medio del cual se asegura la eficacia de los contratos realizados por vía telemática. Además, en su apartado segundo hace una exclusión de este precepto a los siguientes tipos de contrato: los de creación o transferencia de derechos en materia inmobiliaria salvo los de arrendamiento, los que requieren de la intervención de los tribunales, autoridades o profesionales de sector público, los de crédito y caución así como las garantías

presentadas por personas que actúan por motivos ajenos a su actividad económica, negocio o profesión y por último los contratos de derecho civil, en concreto Derecho de familia y derecho de sucesiones *(Directiva 2000: art. 9.2).*

Para que el art. 9 tenga sentido, hay que entender también el art. 11 titulado *Realización de un pedido*, en el que se hace referencia a los principios que han de ser aplicados por los Estados miembros siempre que las partes que no son consumidores acuerden lo contrario. Estos principios son los siguientes: el deber de acusar recibo del pedido por parte del prestador de servicios al destinatario sin ningún retraso y por vía electrónica. Se considera que se han recibido tanto el pedido como el acuse de este cuando las partes que lo reciben tengan acceso a los mismos.

Además, en el apartado 2, expresa con la misma excepción que en el primero, que los Estados miembros garantizarán que los medios técnicos sean puestos a disposición del destinatario del servicio por parte del prestador de los mismos, siendo estos medios apropiados, eficaces y accesibles que permitan identificar y corregir los errores de introducción de datos, antes de realizar el pedido.

Finalmente, el apartado 3 de este artículo hace una aclaración indicando que en caso el caso en el que el contrato sea celebrado por intercambio de correo electrónico o cualquier otra comunicación individual que se asemeje, no será necesario el acuse de recibo ni la puesta a disposición del destinatario de los servicios referidos en el párrafo anterior *(Directiva 2000 art. 11).*

Todo esto supone el trasvase de una ingesta cantidad de datos personales que de un modo u otro tienen que ser almacenados y protegidos con la debida diligencia. Por ello el art. 14 titulado *Alojamiento de datos* regula la preservación de los mismos estableciendo la obligación que tienen los Estados miembros de garantizar que el prestador de servicios no sea considerado responsable de los datos facilitados y almacenados por (petición) el destinatario del servicio cuando son almacenados debido a la prestación de un servicio de la sociedad de la información siempre que se cumplan las siguientes condiciones: que el prestador de servicios no tenga conocimiento de la actividad ilícita y, en el caso de una acción por daños y perjuicios, tampoco tenga conocimiento de hechos o circunstancias por los que se revele el

carácter ilícito, o en caso de tener conocimiento de lo anterior, actúe de manera efectiva para eliminar los datos o impedir el acceso a ellos.

No obstante, indica el apartado segundo de este artículo que lo anterior no será de aplicación cuando el destinatario del servicio se encuentre bajo mandato de autoridad o control del prestador de servicios.

Concluye en su apartado tercero, con la posibilidad de que un tribunal o una autoridad pública, de acuerdo con la normativa de los Estados miembros, pueda exigir al prestador de servicios poner fin a una infracción o impedirla, e incluso los Estados miembros podrán establecer procedimientos por los que se lleve a cabo la retirada de datos o la prohibición a su acceso *(Directiva 2000: art. 14)*

Por todo ello, para poder cumplir de manera correcta con lo dispuesto en esta Directiva en el art. 16 titulado *Códigos de conducta* establece que los Estados miembros y la Comisión ayudarán a que se elaboren códigos de conducta a nivel comunitario, al envío voluntario a la Comisión de los proyectos de códigos de conducta, a la posibilidad de acceder a estos códigos electrónicamente en las lenguas comunitarias, a la comunicación de la evaluación de la aplicación de sus códigos de conducta y su repercusión en las prácticas, usos o costumbres relacionados con el comercio electrónico y a la elaboración de códigos de conducta relativos a la protección de los menores y de la dignidad humana.

En el apartado segundo establece que los Estados miembros y la Comisión fomentarán la participación de los consumidores por medio de sus representantes en cuanto a la redacción y aplicación de los códigos de conducta que vean afectados sus intereses, y serán elaborados conforme a lo dispuesto al inicio del apartado 1. Además, cuando sea necesario se consultará a las asociaciones representantes de *“discapacitados y malvidentes” (Directiva 2000: art. 16).*

No obstante, al igual que se regulan aspectos formales o normas dispositivas, también hay cabida para aspectos disciplinarios. En el art. 17 se regula la *solución extrajudicial de litigios* bajo este mismo título, por medio del cual son los Estados miembros los encargados de velar por el cumplimiento, así como de alentar, a los órganos encargados de ello, de actuar contra las prácticas contrarias al ordenamiento,

estableciendo que, en caso de desacuerdo entre el prestador de servicios de la sociedad de la información y el destinatario de este, la legislación del Estado no será inconveniente para el empleo de los mecanismos de solución extrajudicial, que además alentarán a los órganos responsables de la solución extrajudicial de litigios, en concreto de materia de productos de consumo, a que actúen proporcionando garantías de procedimiento adecuadas a las partes afectadas. En última instancia, indica que los Estados miembros incitarán a los órganos responsables de la solución extrajudicial de litigios a que informen a la Comisión de las decisiones más relevantes que tomen en relación con los servicios de la sociedad de la información y que le transmitan el resto de los datos sobre prácticas relacionadas con el comercio electrónico.

Además de estas soluciones extrajudiciales de litigios, el art. 18 exige a los Estados miembros la adopción de medidas de manera rápida e incluso provisional por medio de los recursos judiciales de la legislación nacional respecto a esta materia regula el empleo de los recursos judiciales nacionales**.**

De otro lado, en el art. 19 se regula la *Cooperación entre Estados* indicando que además de cooperar unos con otros, facilitarán tanto ayuda como información cuando les sean solicitadas por otro Estado miembro o la Comisión*,* creando además puntos de contacto accesibles como mínimo por vía electrónica que permitirán que tanto destinatarios como prestadores de servicios acudan para obtener información general sobre cualquier asunto relacionado con la materia así como la obtención de datos de las autoridades, asociaciones y organizaciones de las que pueden obtener información adicional o asistencia práctica

Para concluir, el art. 20 regula que los Estados miembros determinarán las sanciones que han de aplicarse a las infracciones de las disposiciones nacionales adoptadas conforme a esta directiva y ejercerán las medidas pertinentes para que sea aplicable. Estas sanciones deberán de ser "*efectivas, proporcionadas y disuasorias." (Directiva 2000: arts. 18 - 20).*

5. PROTECCIÓN DE DATOS EN CIBERSEGURIDAD

5.1. DATOS PERSONALES

Toda información perteneciente a una persona física viva identificada o identificable es lo que se conoce como datos personales. Además de esto, la cantidad de información recopilada que ayuda a identificar a las personas, también se consideran como tal.[11]

Por persona física viva identificada o identificable entiende el Reglamento General de Protección de datos[12] (en adelante RGPD) a:

> *toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona (RGPD 2016: art. 4.1).*

La Ley Orgánica 3/2018 de Protección de Datos Personales y garantía de los derechos digitales[13], también distingue entre los distintos tipos de información al igual que el RGPD estableciendo que la información puede ser de varios tipos: de carácter numérico, alfabético, fotográfico, acústico o de cualquier otro tipo relativa a personas físicas, tanto a su identidad como a su existencia y ocupaciones.

Además, los datos personales pueden ser anonimizados, cifrados o presentados con un seudónimo, y aun así seguir considerándose datos personales que se inscriben en el ámbito de aplicación del RGPD. No obstante, si esta anonimización desvirtúa la personalidad de los datos, no tiene sentido seguir considerándolos datos personales, por lo que perderían este atributo.

En cuanto al derecho a la intimidad en relación con el uso de datos personales, el RGPD establece como pilar fundamental, la protección de las personas físicas en

---

[11] Esta definición de datos personales ha sido extraída de la página web oficial de la Unión Europea https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_es

[12] Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos)

[13] La Ley Orgánica 3/2018 de Protección de Datos Personales y garantía de los derechos digitales fue aprobada por las Cortes Generales y sancionada por el S.M el Rey Felipe VI el 5 de diciembre de 2018.

lo que al uso de sus datos se refiere. Además, para ello recurre a dos preceptos legales de ámbito internacional como son el art. 8.1 de la Carta de los Derechos Fundamentales de la Unión Europea (en adelante Carta), y el art. 16.1 del Tratado de Funcionamiento de la Unión Europea (en adelante TFUE), que establecen que *"toda persona tiene derecho a la protección de los datos de carácter personal que le conciernen" (TFUE 1957: art. 16.1).*

Si extrapolamos estas normas internacionales a la regulación legal española nos encontramos con el art. 18.4 CE donde se establece 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 (Constitución Española 1978: art. 18.4).* La importancia de este derecho a la intimidad se debe a que constituye un derecho fundamental inherente a la persona y que por tanto debe ser protegido con la mayor diligencia posible.

Tal es así que en el año 2018, la Sala Primera del Tribunal Constitucional en su sentencia 58/2018, de 4 de junio[14] estimó parcialmente el recurso de amparo

[14] En los años ochenta el Periódico "El País", publicó en su edición impresa, el desmantelamiento de una red de tráfico de estupefacientes, en la que se hallaba implicado el familiar de un destacado cargo público identificado con nombre y apellido. En la noticia se describía la manera de actuar que tenía la red, el ingreso en prisión de los partícipes y la condición de toxicómanas de las personas recurrentes. En 2007 el periódico permitió el acceso gratuito a su hemeroteca digital (www.elpais.com). Por ello, al introducir el nombre y apellido de los recurrentes en amparo en Internet, aparecía la noticia como primer resultado de búsqueda. Cuando los familiares del afectado tuvieron conocimiento de estos hechos, solicitaron al periódico "El País" el cese del tratamiento de estos datos personales, o en su defecto que el nombre y apellido fuese sustituido por las iniciales. Sin embargo, el diario, basándose en su derecho fundamental a la libertad de información y en la imposibilidad de evitar la indexación por los buscadores, no accedió a la solicitud, propiciando la apertura de la vía judicial. Hechas las alegaciones de las partes, el Juzgado de Primera Instancia núm. 21 de Barcelona dictó sentencia, en fecha de 4 de octubre de 2012, que estimó íntegramente la demanda. La resolución consideró probado que «El País» no había adoptado mecanismos de control para evitar la indiscriminada difusión de la noticia. El tribunal condenó a la editorial, al abono de una indemnización, al cese inmediato en la difusión de la noticia y a la implantación de las medidas tecnológicas solicitadas en la demanda, adecuadas para evitar que la información fuera hallada cuando se insertaban en Google los nombres y apellidos de las personas actoras.
El "El País" interpuso recurso de apelación ante la Sección Decimocuarta de la Audiencia Provincial de Barcelona, de 11 de octubre de 2013. Mantenía los motivos de la contestación a la demanda de instancia y añadió además la improcedencia de la cuantía de la indemnización. Los demandantes se opusieron al recurso e impugnaron la Sentencia de primera instancia al considerar que había incurrido en incongruencia omisiva respecto de las pretensiones de la demanda. la Sección Decimocuarta de la Audiencia Provincial de Barcelona dictó sentencia desestimando el recurso y estimando la impugnación de las personas demandantes.

interpuesto por dos individuos contra la Sentencia de 15 de octubre de 2015 de la Sala de lo Civil del Tribunal Supremo, dictada en el recurso de casación núm. 2772-2013 y contra la providencia de la misma Sala, de 17 de febrero de 2016, considerando que se había vulnerado el derecho al honor, a la intimidad y a la protección de datos de carácter personal (art. 18.1 y 4 CE).

5.2. CIBERSEGURIDAD

La ciberseguridad, también denominada seguridad informática es una rama de la seguridad que se focaliza en el campo de la informática y la telemática, protegiendo la información contenida en un computador o aparato informático de las malas práctica conocidas como ciberataques.

Por ciberataque entiende el Instituto Español de Estudios Estratégicos el cibercrimen, el ciberterrorismo e incluso la ciberguerra. Estos tres conceptos tienen en común el ataque premeditado contra una base electrónica. El cibercrimen se centra más en atacar a particulares por medio del robo, fraude, chantaje e incluso falsificación mientras que el ciberterrorismo tiene como objetivo atacar a determinados grupos sociales siempre por medio de la red. En cuanto a la ciberguerra se trata de una confrontación entre estados por medio de la red *(Ureña Centeno, F. 2015).*

No obstante, antes de entrar a tratar el ámbito de la seguridad informática hay que hacer una distinción entre este concepto y el de seguridad de la información, ya que, pese a que en ocasiones se confunden, son definiciones diferentes.

Por ello es necesario hacer una aclaración al respecto de estos dos conceptos que se encuentran interconectados:

Contra esta última Sentencia, Ediciones El País interpuso recurso de casación, alegando de nuevo la caducidad de la acción ejercitada por las personas recurrentes y la inexistencia de vulneración alguna de los derechos al honor, la intimidad y a la protección de datos personales. El recurso fue parcialmente estimado por Sentencia del Tribunal Supremo, de 15 de octubre de 2015.
Tras este largo proceso judicial, los demandantes interponen recurso de amparo ante la Sala Primera del TC concluyendo éste con una estimación parcial del recurso.

De un lado la ISOTools Excellence[15] (2017) se refiere a la seguridad informática de la siguiente manera:

> *La seguridad informática protege el sistema informático, tratando de asegurar la integridad y la privacidad de la información que contiene. Por lo tanto, podríamos decir, que se trata de implementar medidas técnicas que preservarán las infraestructuras y de comunicación que soportan la operación de una empresa, es decir, el hardware y el software empleados por la empresa.*

De otro lado los consultores en Seguridad de la Información (2016), entienden la seguridad de la información como *el área de la informática que consiste en asegurar que los recursos del sistema de información (material informático o programas) de una organización, sean utilizados de manera correcta*.

Hecha esta aclaración, la ciberseguridad consiste en lo que el Doctor Jeimy J. Cano[16] define como seguridad informática. Por ello, podría entenderse la seguridad informática como la base o el pilar de la seguridad de la información, es decir, la creación de las herramientas necesarias para llevar a cabo la seguridad de la información requerida en este ámbito.

Así pues, la seguridad informática se centra en tres tipos de ciberseguridad en función del elemento objeto del ataque. Esto se debe a que en el mundo cibernético nos encontramos con tres factores fundamentales que son los que se ven afectados por los ciberataques: la red o comúnmente conocida como Internet, el software o aplicaciones informáticas encargadas de desarrollar todo el entramado que hay detrás de un computador y por último el hardware, que es la parte tangible de un computador.

---

[15] *IsoTools Excellence* es una empresa encargada de administrar Sistemas de Gestión y Modelos de Excelencia formado por un conjunto de diferentes módulos, dando lugar así, a un software flexible, escalable y adaptable a las diferentes particularidades y necesidades de cada organización**,** con independencia del tamaño o sector en el que cada una se encuadre.

[16] Jeimy J. Cano es Ingeniero y Magíster en Ingeniería de Sistemas y Computación (Universidad de los Andes). Especialista en Derecho Disciplinario (Universidad Externado de Colombia). Doctorado en Administración de Negocios (Newport University) y Doctorado en Educación (Universidad Santo Tomás, Colombia). Posee más de 20 años de experiencia como académico, profesional y ejecutivo en cuestiones de seguridad de la información, privacidad, ciberseguridad, sistemas de información, gobierno y auditoría de TI.

Por ello, los tres tipos de ciberseguridad[17] son los siguientes:

Seguridad de red**:** esta seguridad podría definirse como una seguridad generalizada. Es decir, intenta proteger la información contenida en la red y a la que es accesible cualquier persona a través de internet. Protege a los usuarios de los ciberatacantes que intentan acceder a sus datos por medio de amenazas tales como virus, troyanos o phising[18] entre otros.

Los mecanismos más comunes para combatir ataques a la red son los antivirus, cortafuegos y redes privadas para acceder de manera más segura a la red.

Seguridad de software: esta seguridad se encarga de proteger, valga la redundancia, el software, que como he explicado anteriormente lo componen las aplicaciones encargadas de desarrollar todo aquello que existe detrás de un computador y que es lo que permite que este funcione con normalidad. Para llevar a cabo esta protección, el método más empleado son los programas antivirus. Estos programas se instalan en los computadores y se actualizan de manera automática para hacer frente a los virus que intentan atacar a este tipo de sistema informático.

Seguridad de hardware: el hardware es la parte tangible de un sistema informático. Por tanto, la seguridad de hardware consistirá en la protección de la misma, es decir, el dispositivo en general. Para ello se lleva a cabo el empleo de cortafuegos. Este método de seguridad es inherente a los sistemas informáticos y se basa en limitar el acceso no autorizado a los distintos computadores que se encuentran conectados a una red.

[17] Estos tipos de seguridad han sido extraídos de la siguiente fuente online: ICEMD ESIC. *Tipos de seguridad informática, ¿cuáles existen?* [en línea] Disponible en .<https://www.viewnext.com/tipos-de-seguridad-informatica/https://www.icemd.com/digital-knowledge/articulos/tipos-de-seguridad-informatica-cuales-existen/> [15 diciembre 2019]

[18] El phishing es el término informático utilizado para hacer referencia a lo que se conoce más comúnmente como suplantación de identidad, por medio de la adquisición de información confidencial de manera fraudulenta.

5.3. PROTECCIÓN DE DATOS

Para llevar a cabo la correcta protección de los datos personales en el mundo cibernético, es necesario acudir al Reglamento (UE) 2016/679 Del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos). Esta regulación es de ámbito internacional (UE), lo que supone que será de aplicación para todos los Estados miembros. En lo que respecta al ámbito nacional, nos encontramos con la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. No obstante, debido a que las transacciones electrónicas son en su mayoría de carácter internacional, nos centraremos en el Reglamento general de protección de datos.

5.3.1. Regulación europea. El Reglamento General de Protección de Datos (Reglamento 2016/679)

El Reglamento General de Protección de Datos (Reglamento 2016/679) fue publicado en el Diario Oficial de la Unión Europea el 4 de mayo de 2016. Tiene como objeto la protección de los datos personales por tratarse de un Derecho Fundamental como ya se ha explicado supra, tal y como se regula en la Carta de los Derechos Fundamentales de la Unión Europea en su art. 8.1 y en el art. 16.1 del TFUE.

Por ello, la UE crea este Reglamento, para unificar la protección de los datos personales a nivel europeo y que sea igual en todos los Estados miembros, además de regular las obligaciones del responsable del tratamiento de estos datos[19] y los derechos de las personas físicas.

El RGPD contiene 99 artículos que lo desarrollan. Estos artículos se encuentran subdivididos en capítulos que los contienen, concretamente son 11 que a su vez están de nuevo subdivididos en secciones de la siguiente manera:

[19] El responsable del tratamiento de los datos personales encuentra su definición en el art. 3 del presente Reglamento.

- Capítulo I. Disposiciones generales.
    - ❏ Arts. 1 - 4
- Capítulo II. Principios.
    - ❏ Arts. 5 - 11
- Capítulo III. Derechos del interesado.
    - ➢ Sección 1. Transparencia y modalidades.
        - ❏ Art. 12
    - ➢ Sección 2. Información y acceso a los datos personales.
        - ❏ Arts. 13 - 15
    - ➢ Sección 3. Rectificación y supresión.
        - ❏ Arts. 16 - 20
    - ➢ Sección 4. Derecho de oposición y decisiones individuales automatizadas.
        - ❏ Arts. 21 - 22
    - ➢ Sección 5. Limitaciones
        - ❏ Art. 23
- Capítulo IV. Responsable del tratamiento y encargado del tratamiento
    - ➢ Sección 1. Obligaciones generales
        - ❏ Arts. 24 - 31
    - ➢ Sección 2. Seguridad de los datos personales
        - ❏ Arts. 32 - 34
    - ➢ Sección 3. Evaluación de impacto relativa a la protección de datos y consulta previa
        - ❏ Arts. 35 - 36

- ➢ Sección 4. Delegado de protección de datos
    - ❑ Arts. 37 - 39
- ➢ Sección 5. Códigos de conducta y certificación
    - ❑ Arts. 40 - 43

- Capítulo V. Transferencias de datos personales a terceros países y organizaciones internacionales
    - ❑ Arts. 44 - 49
- Capítulo VI. Autoridades de control independientes
- ➢ Sección 1. Independencia
    - ❑ Arts. 51 - 54
- ➢ Sección 2. Competencia, funciones y poderes
    - ❑ Arts. 55 - 59
- Capítulo VII. Cooperación y coherencia
- ➢ Sección 1. Cooperación y coherencia
    - ❑ Arts. 60 - 62
- ➢ Sección 2. Coherencia
    - ❑ Arts. 63 - 67
- ➢ Sección 3. Comité europeo de protección de datos
    - ❑ Arts. 68 - 76
- Capítulo VIII. Recursos, responsabilidad y sanciones
    - ❑ Arts. 77 - 84
- Capítulo IX. Disposiciones relativas a situaciones específicas de tratamiento
    - ❑ Arts. 85 - 91
- Capítulo X. Actos delegados y actos de ejecución

- ❏ Arts. 92 - 93

- Capítulo XI. Disposiciones finales

  - ❏ Arts. 94 - 99

Hecho este esquema estructural del RGPD, procedemos al análisis de su contenido en primer lugar con su entrada en vigor.

El art. 99 titulado *entrada en vigor y aplicación* indica que la entrada en vigor del Reglamento tendrá lugar a los 20 días de la publicación de este en el Diario Oficial de la Unión Europea (en adelante DOUE). En cuanto a la aplicación, será a partir del 25 de mayo de 2018, y será obligatorio en su totalidad en todos los Estados miembros.

En cuanto a la finalidad de este, la encontramos en el art. 1 titulado *objeto* donde se establecen las normas referentes a la protección de los datos personales de las personas físicas, protegiendo de este modo el derecho fundamental a la intimidad personal y a los datos personales. Además, en su apartado 3 establece la prohibición de cualquier tipo de restricción de datos de personales en la UE por tratarse de datos de este carácter personal.

Los arts. 2 y 3 hablan del ámbito de aplicación de este Reglamento, haciendo distinción entre el ámbito material y el territorial.

En concreto el art. 2 regula el *ámbito de aplicación material*, indicando que el Reglamento se aplicará al tratamiento automatizado de datos personales ya sea este tratamiento de manera total o parcial, así como al tratamiento no automatizado de datos personales en caso de ser contenidos o incluidos en un fichero.

Además, en su apartado segundo excluye todos aquellos casos de tratamiento de datos personales a los que no le son de aplicación el Reglamento. Estos datos personales excluidos son aquellos cuyo tratamiento se lleva a cabo por una actividad que no se encuentra comprendida en el ámbito de aplicación del Derecho de la Unión, por Estados miembros cuando las actividades que llevan a cabo son las comprendidas

en el capítulo 2 del título V del TUE[20], cuando se lleva a cabo en el ejercicio de actividades estrictamente personales o domésticas, cuando lo ejercen las autoridades competentes con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales e incluso de ejecución de sanciones penales.

El ámbito de aplicación territorial lo regula el art. 3 bajo la rúbrica *ámbito territorial* y establece en su apartado primero que el presente Reglamento será de aplicación al tratamiento de datos personales en lo que respecta a actividades de un establecimiento del responsable o del encargado de la Unión con independencia de que sea en la misma Unión:

Además, extiende la aplicación del Reglamento a los casos en los que el tratamiento de datos personales de interesados que residen en la Unión se hace por parte de un responsable o encargado que no se encuentra establecido en la Unión siempre que las actividades del tratamiento de estos datos se encuentren relacionadas con la oferta de bienes o servicios a esos interesados con independencia de que se les requiera el pago de estos, o el control del comportamiento siempre que sea en la Unión.

Por último, en el apartado tercero indica que el Reglamento será de aplicación también al tratamiento de datos personales por parte de un responsable que no se encuentre establecido en la Unión, pero sí en un lugar en el que sea aplicable el Derecho de los Estados miembros conforme al Derecho internacional público.

Si seguimos con el orden establecido en el Reglamento, el art. 4 titulado definiciones hace una aclaración de los conceptos más importantes que han de ser entendidos para poder aplicar esta disposición legal de manera correcta. Las definiciones que destacar son las siguientes:

> *A efectos del presente Reglamento se entenderá por:*
>
> *1) **«datos personales»**: toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda*

[20] Título V disposiciones generales relativas a la acción exterior de la unión y disposiciones específicas relativas a la política exterior y de seguridad común. Capítulo 2 *disposiciones específicas sobre la política exterior y de seguridad común.*

determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona;

2) ***«tratamiento»****: cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción; (...)*

5) ***«seudonimización»****: el tratamiento de datos personales de manera tal que ya no puedan atribuirse a un interesado sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable; (...)*

7) ***«responsable del tratamiento» o «responsable»****: la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento; si el Derecho de la Unión o de los Estados miembros determina los fines y medios del tratamiento, el responsable del tratamiento o los criterios específicos para su nombramiento podrá establecerlos el Derecho de la Unión o de los Estados miembros;*

8) ***«encargado del tratamiento» o «encargado»****: la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento; (...)*

12) ***«violación de la seguridad de los datos personales»****: toda violación de la seguridad que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos; (...)*

16) ***«establecimiento principal»****:*

a) en lo que se refiere a un responsable del tratamiento con establecimientos en más de un Estado miembro, el lugar de su administración central en la Unión, salvo que las decisiones sobre los fines y los medios del tratamiento se tomen en otro establecimiento del responsable en la Unión y este último establecimiento tenga el poder de hacer aplicar tales decisiones, en cuyo caso el establecimiento que haya adoptado tales decisiones se considerará establecimiento principal;

b) en lo que se refiere a un encargado del tratamiento con establecimientos en más de un Estado miembro, el lugar de su administración central en la Unión o, si careciera de esta, el establecimiento del encargado en la Unión en el que se realicen las principales actividades de tratamiento en el contexto de las actividades de un establecimiento del encargado en la medida en que el encargado esté sujeto a obligaciones específicas con arreglo al presente Reglamento;

*17) **«representante»**: persona física o jurídica establecida en la Unión que, habiendo sido designada por escrito por el responsable o el encargado del tratamiento con arreglo al artículo 27, represente al responsable o al encargado en lo que respecta a sus respectivas obligaciones en virtud del presente Reglamento; (...)*

*21) **«autoridad de control»**: la autoridad pública independiente establecida por un Estado miembro con arreglo a lo dispuesto en el artículo 51;*

*22) **«autoridad de control interesada»**: la autoridad de control a la que afecta el tratamiento de datos personales debido a que:*

a) el responsable o el encargado del tratamiento está establecido en el territorio del Estado miembro de esa autoridad de control;

b) los interesados que residen en el Estado miembro de esa autoridad de control se ven sustancialmente afectados o es probable que se vean sustancialmente afectados por el tratamiento, o

c) se ha presentado una reclamación ante esa autoridad de control; (...) *(RGPD, 2016).*

En cuanto a los principios que rigen este Reglamento, debemos acudir al art. 5 titulado *Principios relativos al tratamiento*, donde se establece que los datos personales habrán de ser tratados lícita, leal y transparentemente. A su vez su uso deberá ser con unos *"fines determinados, explícitos y legítimos".* Además, se deberá aplicar lo que se conoce como *"minimización de datos"* que significa que el uso de estos se emplee sólo y exclusivamente para el fin por el que se usaron los datos. Han de ser datos exactos y actualizados y mantenidos por un periodo de tiempo limitado, garantizando de este modo la seguridad que se merecen.

Por ello nos remitimos de aquí al art. 7 *Condiciones para el consentimiento* ya que el consentimiento de la persona de la que se hacen uso sus datos es primordial en este procedimiento. El responsable del tratamiento de los datos personales tendrá la obligación de demostrar que el interesado en sus datos prestó su consentimiento.

Para concluir con el análisis del contenido de este Reglamento me gustaría hacer referencia a los artículos de este que regulan los derechos de los ciudadanos que se ven protegidos en el Capítulo III bajo la rúbrica *Derechos del interesado*. Estos derechos son los siguientes: derecho a la transparencia de la información, comunicación y modalidades de ejercicio de los derechos del interesado (art.12), derecho a la información que deberá facilitarse cuando los datos personales se obtengan del interesado y cuando no se hayan obtenido de éste (arts. 13 y 14), derecho de acceso del interesado (art. 15), derecho de rectificación (art. 16), derecho de supresión («el derecho al olvido») (art. 17), derecho a la limitación del tratamiento (art. 18), derecho de obligación de notificación relativa a la rectificación o supresión de datos personales o la limitación del tratamiento (art. 19), derecho a la portabilidad de los datos (art. 20) y derecho de oposición (art. 21).

6. UBER: EL ROBO DE DATOS A MILLONES DE USUARIOS

Uber[21] al igual que cualquier empresa que prestas sus servicios haciendo uso de la red[22] se encuentra expuesto al robo de cualquier tipo de información que contiene, tanto al robo de datos personales, como al uso indebido de la información contenida en estos, sufriendo de este modo las consecuencias propias de los ataques cibernéticos que hemos definido en capítulos anteriores.

El caso del robo de datos a Uber ha sido uno de los más sonados por lo que la compañía supone para la sociedad. En primer lugar, por su rápido crecimiento, fue creado en 2009 en San Francisco, California (EE. UU.) y en menos de 1 década ha sido capaz de extender su negocio a más de 65 países.

En segundo lugar, por el mercado en el que opera (medios de transporte), ya que el transporte se considera una necesidad casi inherente a las personas, e incluso

[21] La información contenida en este apartado ha sido extraída de las siguientes fuentes (todas ellas periódicos digitales): (1) https://elfinanciero.com.mx/tech/uber-pagara-multa-historica-por-robo-de-datos, (2) https://www.lavanguardia.com/economia/20180927/452052109717/uber-robo-datos-hackeo-pago.html, (3) https://elpais.com/economia/2018/11/27/actualidad/1543328963_962522.html

[22] Para poder hacer uso de esta aplicación, es necesario en primer lugar descargársela e introducir los datos personales del usuario; nombre y apellidos, número de teléfono y cuenta corriente bancaria.

en cuestiones fiscales, existe la controversia de convertirlo en “primera necesidad” aplicándole de este modo en lugar del tipo de IVA reducido (10%), el superreducido (4%).

Finalmente, Uber cuenta con una posición privilegiada frente a otras empresas, por el servicio que presta. La modalidad con la que opera Uber es una de las que más se acerca a las necesidades de la sociedad en lo que a transporte se refiere. Se trata de una compañía que ofrece un servicio de transporte rápido, efectivo y a un coste económico inferior a la media (en la mayoría de los casos), lo que hace que sea cada vez más demandado por la sociedad, pues cuanta más oferta hay en el mercado mayor es la demanda.

Una vez analizado el *modus operandi* de la compañía, no es de extrañar que sus datos se encuentren expuestos con mayor facilidad que los de otras empresas. Desde 2007 hasta hoy Uber ha prestado sus servicios de manera ininterrumpida. Sin embargo, fue en 2016 cuando sufrió un ataque cibernético (brecha de seguridad)[23] que minó en gran medida su reputación a nivel internacional. No obstante, hasta finales de 2017 no se revelaron los hechos. Uber habría pagado 100.000 dólares a los hackers para evitar que la compañía perdiese posiciones en el mercado. Se conoce el hackeo de 607 mil números de licencia de conducir en EE. UU y decenas de millones de direcciones de correo electrónico y números de teléfono de usuarios. En total fueron 57 millones los clientes de Uber de todo el mundo que se vieron afectados por este robo masivo de datos.

Pese a que los hechos ocurrieron en EE. UU, este ciberataque afectó a millones de usuarios de muchas partes del mundo, entre otras, de Estados miembros de la Unión Europea. Tal es así que la Autoridad Holandesa de Protección de Datos multó a Uber a pagar la cantidad de 600.000€ por haber ocultado el ataque a sus clientes, ya que 174.000 de afectados eran holandeses. Tras el robo, la Autoridad Holandesa

[23] Una brecha de seguridad es lo que define el RGPD como una violación de la seguridad de los datos personales: *“toda violación de la seguridad que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos.”*

de Protección de datos abrió una investigación a nivel europeo por los hechos ocurridos, contando el equipo de investigación con países como Alemania, Francia, Italia y Reino Unido. Por parte de Reino Unido también tuvo su sanción. La multa ascendía a 433.818 euros por "no proteger la privacidad de 2,7 millones de viajeros".

Por ello, es necesario hacer una relación del RGPD y de los hechos expuestos anteriormente por su claridad y regulación al respecto.

En primer lugar, hace caso omiso a lo dispuesto en el art. 32 *Seguridad del tratamiento* (de datos personales), ya que este artículo indica que, el responsable y el encargado del tratamiento de los datos aplicarán las medidas técnicas y organizativas necesarias para garantizar un nivel de seguridad adecuado al riesgo que corren.

Además, actuó en contra del Reglamento, en concreto conforme a lo dispuesto en el art. 33 *Notificación de una violación de la seguridad de los datos personales a la autoridad de control*, al ocultar el robo de los datos y no informar a la autoridad de control competente de acuerdo con el art. 55 *Competencia*[24], del riesgo que corrían los datos personales. A su vez, se ocultó información acerca del robo de datos a los clientes (principales afectados de los hechos), lo que también supuso la violación del Reglamento en su art. 34 *Comunicación de una violación de la seguridad de los datos personales al interesado.*[25]

---

[24] Art. 55: *"1. Cada autoridad de control será competente para desempeñar las funciones que se le asignen y ejercer los poderes que se le confieran de conformidad con el presente Reglamento en el territorio de su Estado miembro. 2. Cuando el tratamiento sea efectuado por autoridades públicas o por organismos privados que actúen con arreglo al artículo 6, apartado 1, letras c) o e), será competente la autoridad de control del Estado miembro de que se trate. No será aplicable en tales casos el artículo 56. 3. Las autoridades de control no serán competentes para controlar las operaciones de tratamiento efectuadas por los tribunales en el ejercicio de su función judicial."*

[25] Art, 34 *"1. Cuando sea probable que la violación de la seguridad de los datos personales entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento la comunicará al interesado sin dilación indebida. 2. La comunicación al interesado contemplada en el apartado 1 del presente artículo describirá en un lenguaje claro y sencillo la naturaleza de la violación de la seguridad de los datos personales y contendrá como mínimo la información y las medidas a que se refiere el artículo 33, apartado 3, letras b), c) y d). 3. La comunicación al interesado a que se refiere el apartado 1 no será necesaria si se cumple alguna de las condiciones siguientes: a) el responsable del tratamiento ha adoptado medidas de protección técnicas y organizativas apropiadas y estas medidas se han aplicado a los datos personales afectados por la violación de la seguridad de los datos personales, en particular aquellas que hagan ininteligibles los datos personales para cualquier persona que no esté autorizada a acceder a ellos, como el cifrado; b) el responsable del tratamiento ha tomado medidas ulteriores que garanticen que ya no exista la probabilidad de que se concretice el alto riesgo para los derechos y libertades del interesado a que se refiere el apartado 1; c) suponga un esfuerzo*

De otro lado, en EE. UU, 50 fiscalías iniciaron una investigación conjunta, y el resultado fue la imposición de una multa pecuniaria de 148.000 millones de dólares.

Sin embargo, este caso no es la excepción a la regla. El número de ciberataques sufridos por empresas y usuarios están en constante crecimiento, además se llevan a cabo por medio de actuaciones cada vez más intensas e irreparables. No obstante, no es una práctica que se vaya a erradicar con la creación de nuevas herramientas de protección, ya que las herramientas de ataque también evolucionan. Por ello, como dice Spafford[26]: *el único sistema completamente seguro es aquel que está apagado, encerrado en un bloque de cemento y sellado en una habitación rodeada de alambradas y guardias armados.*

desproporcionado. En este caso, se optará en su lugar por una comunicación pública o una medida semejante por la que se informe de manera igualmente efectiva a los interesados. 4. Cuando el responsable todavía no haya comunicado al interesado la violación de la seguridad de los datos personales, la autoridad de control, una vez considerada la probabilidad de que tal violación entrañe un alto riesgo, podrá exigirle que lo haga o podrá decidir que se cumple alguna de las condiciones mencionadas en el apartado 3."

[26] Gene Spafford es profesor estadounidense de informática en la Universidad de Purdue y un destacado experto en seguridad informática.

7. CONCLUSIONES

PRIMERA.- Sin la existencia y creación de una red de computadores por el Departamento de Defensa de Estados Unidos (DOD) bajo las órdenes de DARPA, para que la comunicación entre las diferentes instituciones académicas y estatales fuesen más fluidas, Internet nunca hubiese llegado a existir y con ello el objeto de este trabajo, las transacciones comerciales electrónicas.

Tal es la importancia de este tipo de comercio (electrónico) que se ha hecho una distinción dentro de este en función de quienes son las partes en la transacción, diferenciando así entre el *Business to Business, Business to Consumer* y *Consumer to Consumer.*

SEGUNDA.- Las transacciones comerciales han experimentado un gran avance en los últimos años gracias a la tecnología de red, dando lugar a lo que se conoce como transacciones comerciales electrónicas, que adoptan un término más técnico bajo el concepto de *e-commerce.* El avance de esta modalidad de comercio ha supuesto tal crecimiento para la sociedad de la información que, paralelamente se han ido desarrollando y evolucionando los delitos informáticos conocidos como ciberataques.

TERCERA.- el Instituto Español de Estudios Estratégicos define el ciberataque como el cibercrimen, el ciberterrorismo e incluso la ciberguerra. Todos ellos tienen en común la manera de combatirlos. Nace aquí la *seguridad informática*, encargada de proteger la información contenida en la red y de la que derivan los tres tipos principales de seguridad: la seguridad de red, la seguridad de software y la seguridad hardware.

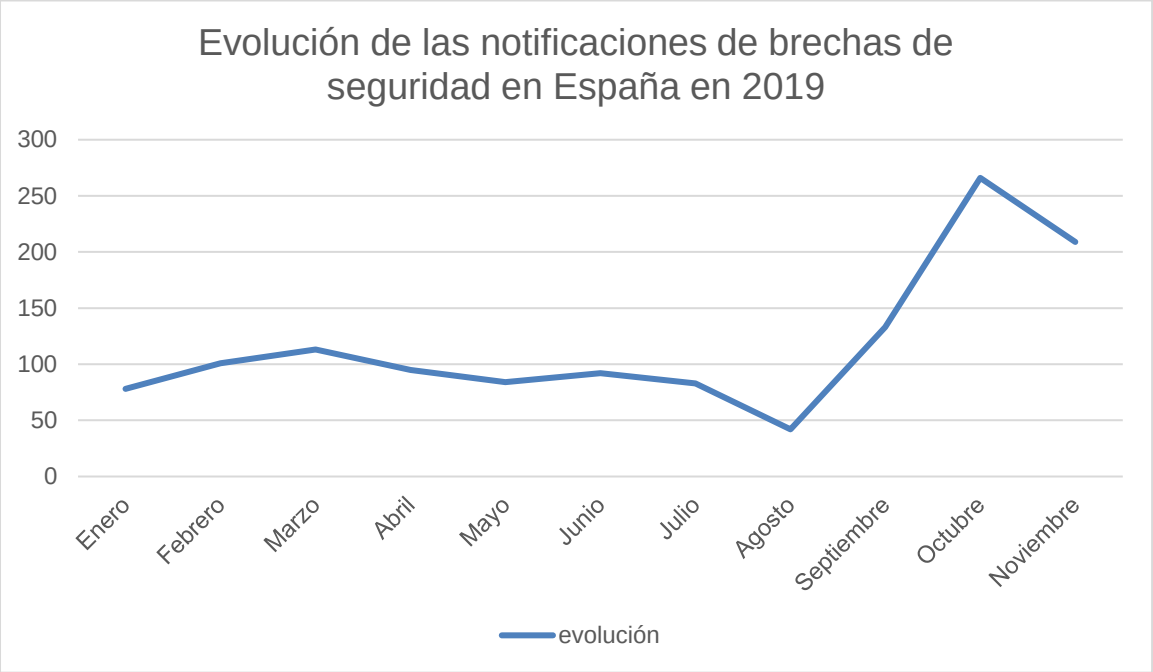
CUARTA.- Toda esta evolución tecnológica y la manera en que la sociedad se adapta e interactúa con ella es lo que se conoce como sociedad de la información. No obstante, pese a que este término se acuña con la creación de Internet, no se ciñe sólo al mismo, sino también a la facilidad del acceso e intercambio de información y datos. De aquí nace la Directiva 2000/31/CE relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior, con el objetivo de mejorar el *e-commerce*,

regulando el funcionamiento del mercado interior y garantizando la libre circulación de información dentro de la UE.

QUINTA.- Los datos personales objeto del *e-commerce* requieren de una protección especializada en *los datos de carácter personal* que los usuarios y clientes de las empresas (páginas web) “ceden” a estas en el momento en el que *clican* una pestaña que “obliga” a *aceptar políticas de privacidad.* Por ello en mayo de 2016 se publica en el DOUE el RGPD cuyo principal objetivo además de la protección de los datos personales es la unificación de esta protección en los países miembros de la UE, siendo aplicable a cada Estado Miembro sin necesidad de llevar a cabo la trasposición previa.

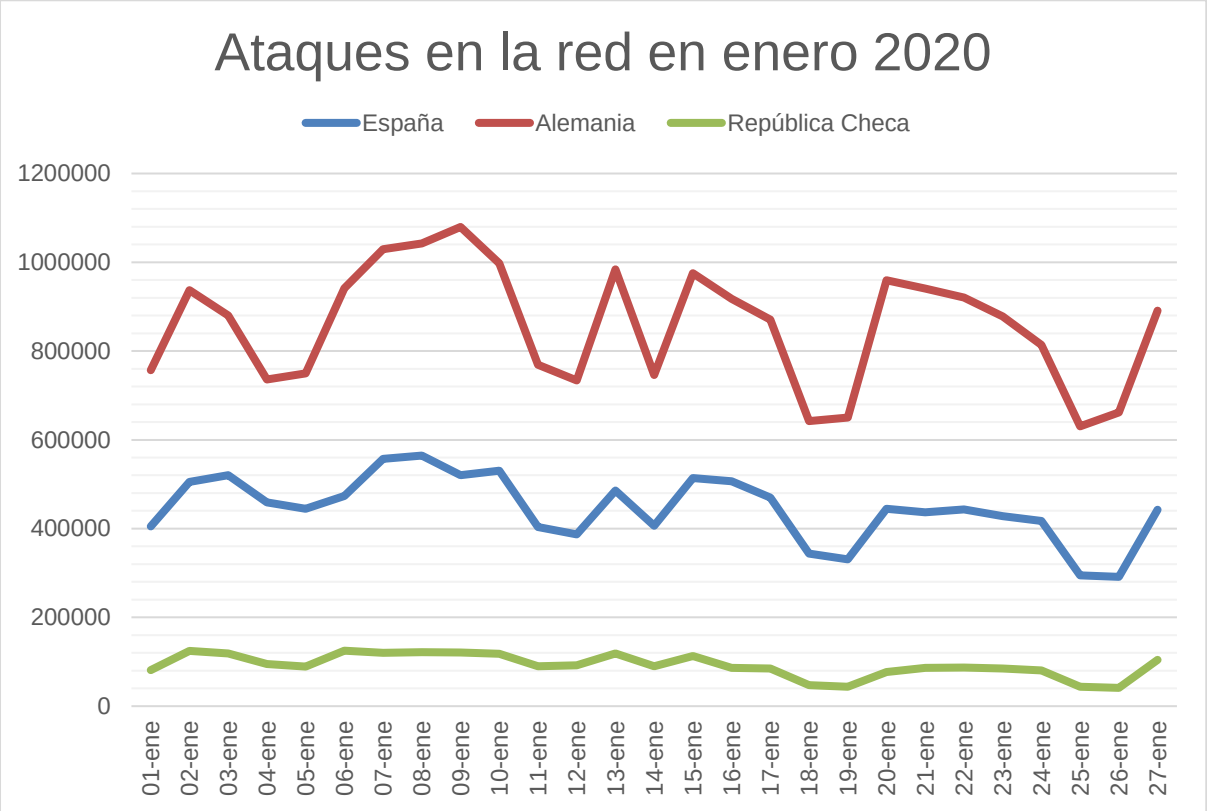
8. ANEXOS

ANEXO I. Gráfica de la evolución de las notificaciones de brechas de seguridad en España (2019).



Fuente elaboración propia. Datos extraídos de: <https://bitlifemedia.com/2020/01/mayores-brechas-datos-seguridad-2019-actualizadas/>

ANEXO II. Gráfica comparativa de los ataques en las redes en enero 2020



Fuente elaboración propia. Datos extraídos de:

<https://cybermap.kaspersky.com/es/stats/#country=86&type=ids&period=m>

9. BIBLIOGRAFÍA

- **Doctrina**

- Alonso, A. (2004) *Comercio Electrónico: Antecedentes, fundamentos y estado actual*. España: Madrid: Dykinson.
- Cotino, L. (2008) *Consumidores y usuarios ante las nuevas tecnologías.* España: Valencia: Tirant Lo Blanch.
- De Miguel, P. Capítulo II (2008) *El Consumidor ante la contratación electrónica internacional. Mercado global y protección de los consumidores*: *Consumidores y usuarios ante las nuevas tecnologías.* Ed por Cotino, L. Valencia: Tirant Lo Blanch.
- Del Peso, E. (2003). *Servicios de la sociedad de la información. Comercio electrónico y protección de datos.* Madrid: Díaz de Santos.
- Fueyo, D. (2010). *Programar para el aula en la etapa de educación primaria* LOE, Lulu, Oviedo.
- Seoane, E. (2005) *La nueva era del comercio electrónico: Historia del comercio electrónico*. España: Vigo.
- Martínez, J., Rojas, F. (2006) *Comercio Electrónico*. España: Paraninfo.
- Real Academia de la Lengua (1992). *Diccionario de la Lengua Española*. Vigésima primera edición.
- Schneider, G. (2004) *Comercio electrónico: Comercio tradicional.* México: Thomson.

- **Libros electrónicos**

- Ureña Centeno, F (2015). *Ciberataques, la mayor amenaza actual:* Instituto Español de Estudios Estratégicos [en línea] disponible en <http://www.ieee.es/Galerias/fichero/docs_opinion/2015/DIEEEO09-2015_AmenazaCiberataques_Fco.Uruena.pdf> [20 noviembre 2019].

- Schneider, G (2011). *Electronic Commerce* [en línea] disponible en <https://www.cengagebrain.co.uk/shop> [15 enero 2020].

- **Revistas electrónicas**

- Figueroa-Suárez, J., Rodríguez -Andrade, R., Bone-Obando, C. y Saltos-Gómez, J. (2017) "La seguridad informática y la seguridad de la información". *Polo del Conocimiento* [en línea] disponible en <https://polodelconocimiento.com/ojs/index.php/es> [19 enero 2020].

- **Legislación y jurisprudencia.**

- Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.
- Ley Orgánica 3/2018 de Protección de Datos Personales y garantía de los derechos digitales.
- 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.
- Sentencia del Tribunal Constitucional (Sala Primera) de 7 de julio de 2018 ECLI: ES: TC: 2018: 58.

- **Páginas web**

- Consultores en Seguridad de la Información. (2016). *Seguridad Informática vs Seguridad de la Información*. [en línea] disponible en <https://www.maestrodelacomputacion.net/seguridad-informatica-seguridad-de-la-informacion/> [08 diciembre 2019].
- Ecommerce – land Company (2004) *E-commerce – land* [en línea] disponible en <https://www.ecommerce-land.com/history_ecommerce.html> [16 noviembre 2019].

- Instituto Español de Estudios Estratégicos (1970). *Instituto Español de Estudios Estratégicos* [en línea] disponible en <http://www.ieee.es/> [10 enero 2020].
- ISOTools Excellence. (2017) *¿Seguridad informática o seguridad de la información?* en línea] disponible en <https://www.pmg-ssi.com/2017/01/seguridad-de-la-informacion/> [06 diciembre 2019].
- Organización Mundial del Comercio (1995). Programa de trabajo adoptado por el Consejo General el 25 de septiembre de 1998. [en línea] disponible en <https://www.wto.org/spanish/tratop_s/ecom_s/wkprog_s.htm> [13 noviembre 2019].
- Unión Europea (1993). *Web oficial de la Unión Europea* [en línea] disponible en <https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_es> [03 noviembre 2019].