Paula Collado Ricomà

BRECHAS DE SEGURIDAD Y PROTECCIÓN DE DATOS PERSONALES.

TRABAJO DE FINAL DE GRADO DE DERECHO

Dirigido por el Dr. Jaume Vernet

UNIVERSITAT ROVIRA I VIRGILI

Tarragona

2021

Este TFG se ha desarrollado con la modalidad de:

Trabajo de Investigación.

La Investigación se presenta siguiendo la elección de revista y normas de estilo para los autores.

Simulación de juicio.

Dictamen/Informe

APS

La entidad a la que se presenta servicio es.....

TFG vinculado a las practicas.

El sitio en donde se ha desarrollado las prácticas es.....

RESUMEN

Este trabajo de Fin de Grado muestra un estudio detallado de las Brechas de Seguridad en el ámbito de la Protección de Datos, desde un enfoque práctico y siguiendo la modalidad de Informe Jurídico. Este estudio tiene como principal objetivo dar respuesta jurídica a las preguntas planteadas y que hacen referencia al cumplimiento de las obligaciones legales en el caso de incidencias de seguridad que afecten a datos de carácter personal.

RESUM

Aquest treball de Final de Grau mostra un estudi detallat de les Bretxes de Seguretat en l'àmbit de la Protecció de Dades, des de un enfocament pràctic i seguint la modalitat d'Informe Jurídic. Aquest estudi te com a principal objetiu donar resposta jurídica a les preguntes plantejades i que fan referencia al compliment de les obligacions legals en el cas de incidencies de seguretat que afecten a dades de carácter personal.

ABSTRACT

This Final Degree project shows a detailed study of the Security Breaches in the field of Data Protection, from a practical approach and following the Legal Report modality. The main objective of this study is to provide a legal answer to the questions posed and which refer to compliance with legal obligations in the case of security incidents that affect personal data.

PALABRAS CLAVE - KEY WORDS

a) Brecha de seguridad→ Security Breach.

b) Protección de Datos→ Data Protection.

c) Autoridades de Control→ Control Authorities.

d) Delitos Informáticos→ Computer Crimes.

e) Delegado de Protección de Datos→ Data Protection Officer.

INTRODUCCIÓN.

El presente trabajo versará sobre las Brechas de Seguridad y Protección de Datos Personales.

La elección del tema no ha sido al azar; tras reflexionar sobre las distintas opciones que tenía encima de la mesa, finalmente me incline por este tema, por tratarse de un asunto actual y de máxima relevancia, por el continuo avance de las nuevas tecnologías, el desarrollo tecnológico y el uso imparable de Internet.

Por tanto, ha nacido una nueva era, la tecnológica, que se ha colado en nuestras vidas de manera arrolladora para quedarse. En nuestro entorno es difícil actualmente concebir a alguien sin un teléfono móvil o sin un ordenador, todo y así no todas las persones gozan de disponibilidad.

Toda la sociedad conoce estos dispositivos y los usa en su día a día, y es justo reconocer que en algunos aspectos nos han facilitado la vida, a pesar de que en ocasiones nos han hecho esclavos de estos, porque somos incapaces de desprendernos de ellos.

Es importante manifestar en este sentido, las nuevas tecnologías también escoden ciertos peligros, situaciones que en general, las personas acostumbramos a desconocer, y que suponen comportamientos poco precavidos, cuando nos relacionamos con las tecnologías y el Internet, al navegar por páginas web poco seguras, al guardar contraseñas sin revisar las políticas de privacidad y al pagar con nuestros datos, bajo el mantra de que es gratis. Estos comportamientos sin duda pueden suponer ciertos problemas.

El presente Trabajo de Fin de Grado sigue la modalidad de Informe Jurídico, según las tipologías establecidas en la asignatura. En este caso, he seguido las indicaciones del Tutor asignado al trabajo y las indicaciones establecidas en la Universidad de cómo debe estructurarse un Informe Jurídico.

Antes de entrar en materia a modo de consideraciones preliminares sobre lo ocurrido, hay que definir que son: Las Brechas de Seguridad y la Protección de Datos.

Una brecha de seguridad es un incidente que afecta a datos de carácter personal, este puede tener un origen accidental o intencionado y además puede afectar a datos tratados digitalmente o en formato papel. En general, se trata de un suceso que ocasiona destrucción, pérdida, alteración, comunicación o acceso no autorizado a datos personales.

La Protección de Datos, es un conjunto de medidas para garantizar y proteger los datos de carácter personal registrados, que sean susceptibles de tratamiento y que constituyen información sobre nuestra esfera privada y sean susceptibles, de ser usados para valorar ciertos aspectos de nuestra personalidad, como nuestros hábitos, relaciones personales y opiniones.

La Empresa TURBOFARMA COMPLET, sufre una intromisión a sus sistemas informáticos a través del correo electrónico del director de logística de la empresa. Este incidente es informado por un trabajador de la sede de Alemania, alertando a las oficinas de Madrid y a partir de este instante se empiezan aplicar protocolos internos que dan un resultado poco satisfactorio en materia de protección de datos, quedando en evidencia la falta de formación en la materia.

Otro motivo por el cual he escogido hacer el trabajo sobre las Brechas de Seguridad, es debido a que actualmente tengo la inmensa fortuna de ser miembro de un despacho de abogados que asesoran en materia de Protección de Datos a empresas clientes.

La finalidad del Informe Jurídico es dar respuesta jurídica a las preguntas que mi cliente me fórmula para la resolución de la Brecha de Seguridad y si se ha actuado bajo el marco jurídico establecido.

El Informe Jurídico se compone de los siguientes apartados:

Encabezamiento, está reservado para indicar los datos del abogado que realizará la redacción del Informe Jurídico y los datos identificativos de la empresa, que solicita asesoramiento legal para resolver las cuestiones que plantea.

Los Antecedentes de Hecho, se describen los hechos tal como han transcurrido, uno por uno y todos los pasos que la empresa ha ido siguiendo a medida que surgen las adversidades

y problemas que han sufrido. Están diferenciados cada uno por un número y un título, para anunciar el contenido de cada apartado.

Los Fundamentos Jurídicos están numerados para individualizar a cada uno de ellos. Se trata de las bases legales y los argumentos que racionalizan y aclaran la interpretación del derecho, y constituyen el pilar fundamental para poder dar respuesta a las preguntas que realiza el cliente previamente.

Para su elaboración de los fundamentos, se sigue el método jurídico, esto es, el análisis de la normativa aplicable y como está a sido interpretada por los Tribunales.

Para terminar el Informe, propone unas conclusiones que dan respuesta a las preguntas del cliente.

Finalmente, además, se aportan como anexos al TFG, la bibliografía utilizada, y un listado de la normativa y de la jurisprudencia que no forman parte del Informe, pero que han servido para su elaboración.

Cabe destacar, que el caso en concreto descrito en dicho informe no es una cuestión real, es un suceso totalmente inventado, a partir de asuntos ya existentes a los que he tenido acceso en el despacho en el que presto mis servicios y casos de mayor envergadura, que

se han hecho mediáticos por diversas circunstancias y que, a partir de estos acontecimientos, he confeccionado el incidente de TURBOFARMA COMPLET, S.L.

El trabajo de final de grado debe versar sobre un tema que te motive, con la finalidad de apuntalar los conocimientos en la materia y poder seguir aprendiendo y formándote.

Agradezco a mi Tutor del Trabajo de Final de Grado todo su soporte y todas sus indicaciones para la realización de un buen trabajo.

INFORME JURÍDICO SOBRE BRECHAS DE SEGURIDAD Y PROTECCIÓN DE DATOS PERSONALES.

A PETICIÓN DE LA EMPRESA TURBOFARMA COMPLET, S.L.

ENCARGADA DE REALIZAR EL DICTAMEN, PAULA COLLADO RICOMÀ

A TARRAGONA 11 DE JUNIO DEL 2021

Por la presente, Paula Collado Ricomà abogada del Ilustre Colegio de abogados de Tarragona realiza el siguiente informe jurídico, a día 20 de abril del 2021 a petición de la empresa TURBOFARMA COMPLET, S.L. para resolver las cuestiones relacionadas con la legalidad de la evaluación y tratamiento interno de la brecha de seguridad y el incumplimiento de la obligación de notificación ante la autoridad de control.

Ante esta situación mi cometido es estudiar detenidamente la problemática del incidente que ha sufrido la empresa TURBOFARMA y contestar a las preguntas que ellos me han formulado para encontrar una solución legal a la empresa.

Las preguntas que TURBOFARMA plantea son las siguientes:

a) ¿El Cliente pregunta si la tramitación y la notificación de la brecha se ha hecho correctamente y ha cumplido con la normativa de protección de datos?

b) ¿Ha realizado el delegado de protección de datos bien sus funciones, de acuerdo con la legalidad vigente?

c) ¿Es posible emprender acciones penales contra los atacantes?

Estas cuestiones serán resueltas explícitamente en los fundamentos II a IV, y serán resumidos en las conclusiones.

Seguidamente expondremos los hechos acreditados, formulados como antecedentes de hecho.

ANTECEDENTES DE HECHO

1. *Presentación de la empresa.*

TURBOFARMA COMPLET, S.L. es la filial española de la farmacéutica del mismo nombre cuya central está en Alemania. Los servicios centrales de Alemania ofrecen cobertura a todas sus filiales en relación con los sistemas informáticos.

2. *Aviso de la intromisión.*

Siendo así, el día 16 de marzo de 2020, el director financiero recibe notificación mediante correo electrónico enviado por el responsable de protección de datos de Alemania, dónde se le informa, que se ha detectado en los servidores del correo electrónico que dan servicio a España, una intrusión en el correo profesional del director de logística Sr AND.

3. *Inicio del protocolo interno de seguridad.*

Puesta en conocimiento la posible brecha de seguridad el responsable de protección de datos de Madrid, este abre un registro interno y lo califica como una incidencia de seguridad de nivel y alcance desconocido.

4. *Posible sospecha de intromisión en los correos electrónicos.*

El responsable de protección de datos, parte de la sospecha que se ha accedido a los correos de la bandeja de entrada, después de haber detectado la contraseña de la cuenta de correo ubicada en el mismo ordenador, por lo que se desconoce si los intrusos tuvieron acceso a los datos de la empresa, en particular a las bases de datos de SAP, que contiene datos de clientes y proveedores, así como a cualquier otro software alojado en los servidores de TURBOFARMA COMPLET.

5. *Se inician los protocolos internos de la empresa.*

El responsable decide poner en marcha los protocolos internos de la empresa, en las que toma las medidas técnicas y organizativas necesarias para ralentizar la intrusión, como también utilizar sistemas de cifrados y cambiando las contraseñas de todos los sistemas de información de la empresa, con el objetivo de tener más tiempo para poder saber el origen y de qué nivel de impacto se trata.

6. *Descarga de todos los correos electrónicos.*

El mismo día 16, los servicios informáticos de TURBOFARMA COMPLET alertados de la incidencia, inician la descarga de todos los correos electrónicos del terminal implicado, para aislarlo del servidor y el día 17 realizan una copia de seguridad y se procede de nuevo al cambio de contraseñas y se monitorizan los correos implicados para prevenir cualquier uso de este.

A primera vista, no apreciaba que la incidencia pudiera tener un impacto muy alto, y, además, gracias a la aplicación de los protocolos a tiempo, parecía que la brecha no se hubiera materializado.

7. *Cambio de contraseñas.*

Así que, hechos los cambios por lo que hace a la seguridad de las contraseñas del correo electrónico, el responsable de Protección de Datos de Madrid informa al responsable de Alemania que estará atento a cualquiera otra intrusión pero que desde su punto de vista se trataba de un incidente de poca trascendencia, en la que no hacía falta realizar notificación alguna a la autoridad de control, al tratarse de un incidente calificado por el cómo leve. No obstante, se procede a poner en marcha una investigación más detallada.

8. *Inicio a la investigación interna.*

Iniciada la investigación oportuna con la colaboración del director de logística, se contextualiza el origen de la amenaza, en una intrusión externa por acción intencionada, que se materializa en el acceso a los correos electrónicos del director de logística, sin poder confirmar en este momento si hay más cuentas de correo de la compañía involucradas. Además, no se puede descartar el acceso a las bases de datos del SAP (programa dividido por módulos que integra todos los departamentos de una empresa cliente, proveedores) y a cualquier otro software con el que se trabaje.

En este momento de la investigación del incidente, se advierte por primera vez que, la hipótesis inicial referida a una simple intrusión da paso a un problema más grave, ya que podrían estar afectados los contenidos de otros correos electrónicos con datos identificativos, y además, que también podrían haber datos de contacto afectados y, datos bancarios tanto de clientes como proveedores, dado que por esta cuenta se mueve la mayoría de los correos relacionados con la facturación de la compañía.

9. *Listado de los pagos pendientes.*

El día 18 de marzo, el director financiero de la compañía recibe comunicado desde la sede de Alemania, indicándole que debe realizar a la mayor brevedad posible, un listado exhaustivo de los pagos pendientes de adeudo, investigando si se han producido los asientos pendientes en cuenta y en su caso conocer la justificación del retraso, si de momento no se ha producido el pago.

10. *Coordinación de los pagos.*

Ante la petición del director financiero, los trabajadores coordinan con el departamento de logística un listado de los pagos pendientes y, una vez realizado

dicho informe, se da traslado cumplidamente al responsable de protección de datos de Madrid.

11. *Conocimiento de la brecha de seguridad.*

Gracias a la exhaustiva investigación, el director financiero y el responsable de protección de datos de Madrid advierten que el incidente se trata de una brecha grave, y que quizás han demorado más del tiempo que jurídicamente se exige.

En esta situación, se plantean cumplir con lo establecido en la normativa y notificarlo a la Autoridad de Control.

12. *Afectación a 3 farmacias.*

El mismo día, se procede a preparar toda la documentación necesaria para realizar la notificación, y es en ese momento cuando advierten que se han cumplido las 72 horas preceptivas para ponerlo en conocimiento de la Agencia Española de Protección de datos y que se trata de un plazo improrrogable.

En este momento, el director financiero y el responsable de protección de datos pactan que no van a emitir comunicado alguno, a la espera de evaluar como avanzaban los acontecimientos.

13. *Notificación al responsable de protección de datos.*

Un día más tarde, el 19 de marzo, el director financiero constata que ha habido tres farmacias en concreto, que no han realizado los pagos trimestrales. Inmediatamente se realiza una llamada telefónica a cada una de ellas, para conocer cuál era el motivo del retraso en los pagos.

Las tres farmacias coinciden en su respuesta, demostrando documentadamente que ya habían realizado los pagos trimestrales.

14. *Se constatan los pagos de las 3 farmacias*.

En este preciso momento, el director financiero entiende que, el alcance de la brecha de seguridad en el sentido de la peligrosidad potencial del incidente es alto, porque dispone de capacidad para afectar a información valiosa para la empresa y para sus clientes.

La estimación en cuanto a la severidad de las consecuencias es muy alta, dado que las consecuencias pueden ser significativas o incluso irreversibles y lo notifica al responsable de protección de datos, parece que hay tres farmacias clientes, que han sido víctimas de una estafa a causa de la brecha de seguridad que la farmacéutica había sufrido días atrás.

15. *Averiguación que son víctimas de un delito de estafa.*

La documentación, demuestra como las farmacias clientes, efectuaron los pagos de las facturas, en la cuenta que les indicó TURBOFARMA COMPLET antes del vencimiento. En concreto, la farmacia del Mar Menor localizada en la Región de Murcia cuyo importe era de 3.000€. La farmacia Anchos Snack de Madrid cuyo importe era de 5.000€, y por último la farmacia Figuerola de Barcelona que debía pagar una factura de 2.000€.

Los pagos que efectuaron las tres empresas directamente entraron en las cuentas de los atacantes, y esto fue así ya que durante la intrusión habían conseguido hacerse con las contraseñas de los sistemas y también con las contraseñas de sus entidades bancarios dejando así de forma intencionada todas sus cuentas inhabilitadas de forma que los atacantes podían redirigir las cantidades dinerarias a sus propias cuentas.

16. *Intromisión en los sistemas con afectación en los datos.*

También se constata que la intromisión en los sistemas ha supuesto el acceso a datos personales y confidenciales tanto de clientes como de proveedores. En este sentido se estima que podían haber más de 50.000 correos afectados, incluyendo los 3 casos de las farmacias en cuestión, que ya se ha confirmado que han sido víctimas de la brecha de seguridad.

17. *Posible perjuicio de los derechos y libertades de los clientes y proveedores.*

Evidentemente el ataque es mucho mayor de lo que los responsables habían supuesto en un inicio y les preocupa enormemente que por las características del incidente y el tipo de datos referidos, se puedan causar daños a los derechos y libertades de los clientes y proveedores de la farmacéutica cuyos datos están entre los 50.000 correos accedidos en cuestión.

18. *El Sr AND notifica al responsable ciertas irregularidades.*

El 25 de marzo, el Sr. AND advierte irregularidades en sus cuentas bancarias personales, sin que su banco pueda darle explicación alguna.

Al parecer, los atacantes también se hicieron con todas sus credenciales bancarias a pesar de estar guardadas en un programa de cifrado y en general con todo lo que el Sr. AND guardaba en su ordenador. Los movimientos de su cuenta demostraban que se estaba suplantando su identidad y que se estaban realizando posibles contrataciones a su nombre. Esta situación también es puesta en conocimiento del responsable de protección de datos.

19. *Una de las farmacias víctima del atacante.*

A todos los hechos anteriormente mencionados, hay que añadir que, sin haber dado una solución rápida y efectiva a las estafas ni a la suplementación de

identidad del director de logística de la empresa, el día 26 de marzo, es decir al día siguiente, la farmacia Mar Menor notifica a la empresa TURBOFARMA COMPLET que los atacantes se han hecho con parte de sus datos de clientes y que si no efectúan un pago de 8.000 bitcoins antes de los 30 días siguientes filtraran todos los datos, poniendo en peligro la confidencialidad, la integridad y la disponibilidad de los datos de la mencionada farmacia.

20. *Realización del análisis de impacto.*

El responsable de protección de datos realiza el análisis de impacto del riesgo cuantitativo de la brecha de seguridad y lo notifica al responsable de Alemania. Le advierte, que la brecha de seguridad tiene impacto mayor del que esperaban, y fuera de los plazos preceptivos y desbordados por los acontecimientos, solicitan asistencia legal para resolver las dudas y las cuestiones jurídicas de fondo que tienen en la filial de España.

FUNDAMENTOS JURÍDICOS

I

Marco normativo de la Protección de Datos.

A modo preliminar empezamos con un Marco General sobre Protección de Datos. Procede en primer lugar decir, que la **Constitución Española del 1978** no recoge de manera explícita el derecho a la protección de datos. El texto constitucional, en el Capítulo Segundo, Derechos Libertades, en el artículo 18 apartado 4 establece que mediante leyes se limite el uso de la informática en defensa del derecho al honor y a la intimidad personal y familiar de las personas.

Se ha de entender que la protección de datos constituye un derecho autónomo, desligado del honor intimidad y propia imagen, porque su contenido esencial supone, en definitiva, dotar de poder de control al individuo sobre el uso y el destino de sus datos personales.

El Convenio Europeo de los Derechos Humanos del Aprobado por el Consejo de Europa, 4 de noviembre de 1950, establece en el Título I "*Derechos y Libertades"* en concreto en su artículo 8 apartado 1, el derecho al respeto a la vida privada y familiar. Estas obligaciones constituyen el punto de partida del derecho a la protección de datos personales.

También en el ámbito europeo, el **Convenio N.º 108 del Consejo de Europa, de 28 de enero de 1981,** para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, se considera el primer mecanismo a nivel internacional, jurídicamente vinculante en el ámbito de la protección de datos y tiene como objetivo, proteger a las personas contra las intromisiones en su vida privada y contra el uso incorrecto de sus datos personales.

El Tratado de funcionamiento de la Unión Europea, **firmado en Roma,** constituye el texto que contiene con mayor detalle, el marco jurídico de las políticas y acciones de la Unión, a pesar de haber vivido diversas reformas y denominaciones.

Desde la entrada en vigor del **Tratado de Lisboa del 2009**, se le conoce como Tratado de Funcionamiento de la Unión Europea. Dicho texto legal, establece en el Título II "*Disposiciones de Carácter General*" en concreto en el artículo 16 apartado 1, que toda persona tiene derecho a la protección de datos que le concierne. Y en su apartado segundo, que corresponde al Parlamento Europeo y el Consejo establecer, las normas sobre protección de las personas físicas respeto del tratamiento de datos de carácter personal.

Como consecuencia del apartado segundo del artículo 16 citado anteriormente, el Parlamento Europeo y el Consejo en fecha, 24 de octubre de 1995, aprueba la **Directiva 95/46 CE,** relativa a la Protección de Datos de las personas físicas a lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

La presente Directiva, establece que se aplica a los datos tratados por medios automatizados, es decir con base informática, así como a los datos contenidos en ficheros en soporte papel. Del mismo modo también establece que no se aplicará cuando el tratamiento del dato, se circunscriba actividades particulares o domésticas. También lo excluye en los casos de la seguridad pública, la defensa, o la seguridad del Estado.

El artículo 32 de la **Directiva 95/46 de la Unión Europea** establece un plazo de tres años, para la trasposición del contenido de esta, al Ordenamiento interno de los Estados Miembros.

España la traspuso en 1999, tras aprobar la **Ley Orgánica 15/1999** del, 13 de diciembre, de Protección de Datos de carácter personal, (LOPD). Entro en vigor el, 14 de enero del año 2000.

Sin ser una norma específica de protección de datos, la **Ley 9/2014, de 9 de mayo, General de Telecomunicaciones**, contempla de manera explícita en su artículo 41 la exigencia específica del cumplimiento de la Protección de Datos y el respeto a los mismos, referido a la autorización al acceso, al almacenamiento, a la destrucción y a la revelación ilícita. También a la aplicación de políticas de seguridad, como el conjunto de normas de actuación en caso de violación de los datos personales entre las que incluye, la notificación a la Agencia Española de Protección de Datos, como a los particulares sin dilaciones indebidas. La **LGT**, remite a la Ley Orgánica 15/1999.

Igualmente cabe mencionar **la Ley 34/2002 de 11 de julio**, **de Servicios de la Sociedad de la Información y de Comercio Electrónico**, cuyo cuerpo legal se ocupa de la aplicación de la legislación de Protección de Datos a Internet.

En este contexto, cabe citar que con anterioridad a 1999, en España estaba vigente la **Ley Orgánica 5/1992 de 29 de octubre**, de Regulación del Tratamiento Automatizado de Datos de Carácter Personal, (LORTAD). La razón que justifico su aprobación fue la firma en 1999, del Acuerdo de Shengen y del Convenio para su aplicación, relacionado con las ventajas del paso de fronteras y cuyos beneficios los Estado Miembros podrían disfrutar, siempre que implantarán un sistema de protección de datos y una Autoridad de Control, fruto de ello nace la Agencia Española de Protección de Datos en 1992 (AEPD).

El Reglamento UE 2016/679, **del Parlamento Europeo y del Consejo** del, 27 de abril del 2016, relativo a la protección de las personas físicas en los 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, que es conocido como el Reglamento General de Protección de Datos, que entró en vigor el, 25 de mayo de 2016, si bien su aplicación no fue efectiva hasta el, 25 de mayo del 2018.

Este Reglamento se complementa, **con la Directiva (UE) 2016/680, del Parlamento Europeo y del Consejo, de 27 de abril de 2016**, relativa a la protección de las personas físicas en lo que respecto al tratamiento de datos personales por parte de las

autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos, que entró en vigor el, 5 de mayo de 2016, y con el **Reglamento (UE) 2018/1807** del Parlamento Europeo y del Consejo de, 14 de noviembre de 2018, relativo a un marco para la libre circulación de datos no personales en la Unión Europea, que entró en vigor el día, 18 de diciembre de 2018.

Por último, la **Ley orgánica 3/2018**, de 5 de diciembre, de Protección Datos Personales y Garantías de los Derechos Digitales, adapta el Ordenamiento Jurídico Español al RGPD y reconoce un nuevo conjunto de derechos digitales de la ciudadanía, conforme el mandato establecido en el artículo 18.4 de la Constitución del 1978, con especial mención a la neutralidad de la red, el acceso universal a internet, la seguridad digital, la educación digital, y la protección de menores en Internet, así como nuevos derechos digitales en el ámbito laboral de la mano del derecho a la desconexión digital.

El Tribunal Europeo de Derechos Humanos en aplicación del Convenio Europeo de Derechos Humanos de, 4 de noviembre de 1950, ampara el derecho a la protección de los datos en su artículo 8 "*Toda persona tiene derecho al respeto de su vida privada*"
En la Sentencia, 17 de octubre de 2019, *"*Asunto *López Ribalda y otros contra España*" (Demandas N. º1874/13 y 8567/13).

> *"En lo que respecta, más específicamente, a la vigilancia de los empleados en el lugar de trabajo, la Corte ha considerado que el Artículo 8 deja a discreción de los Estados decidir si promulgar o no una legislación específica sobre videovigilancia o la revisión de la correspondencia no profesional y otras comunicaciones de los empleados, No obstante, ha señalado que, independientemente de la discreción de la que gocen los Estados para elegir los medios más adecuados para la protección de los derechos en cuestión, las autoridades nacionales deben garantizar que las medidas de vigilancia que un empleador establezca y que afecten el derecho al respeto de los asuntos privados, la vida privada o la correspondencia de sus*

> *empleados sean proporcionadas y se acompañen de garantías adecuadas y suficientes contra el abuso."*

El alto Tribunal reitera, que el concepto de "vida privada" es un término amplio que no puede ser objeto de una definición exhaustiva. Abarca la integridad física y psicológica de una persona. Por lo tanto, puede abarcar múltiples aspectos de la identidad física y social de la persona y se extiende en particular, a los aspectos relativos a la identidad personal, como el nombre o la imagen de una persona.

En el mismo sentido, el **Tribunal de Justicia de la Unión Europea** en la STJUE de, 13 de mayo de 2014, C- 131/12, en su considerando 10, se manifiesta también sobre el artículo 8 del Convenio Europeo para la Protección de los Derechos Humanos y de las libertades fundamentales, así como en los principios generales del Derecho comunitario, "*considera que las legislaciones nacionales relativas al tratamiento de datos personales tienen por objeto garantizar el respeto de los derechos y libertades fundamentales, particularmente del derecho al respeto de la vida privada".* El objetivo principal es aproximar dichas legislaciones, para asegurar un alto nivel de protección dentro de la Comunidad.

El Tribunal de Justicia, recientemente para la defensa del sistema de garantías del derecho a la protección de datos, en el asunto C-311/18 del 16 de julio del 2020, *Data Protection Comissioner c. Facebook Ireland and Maximillian Schrems.* Ha declarado que la Decisión Escudo de la privacidad es inválida, debido a que las garantías adecuadas, los derechos exigibles y las acciones legales en Estados Unidos, no gozaban de una protección equivalente a lo dispuesto en el RGPD.

En concreto manifiesta:

> *"Sobre la constatación relativa al nivel de protección adecuado habida cuenta de los elementos mencionados por la Comisión en la Decisión EP y de los acreditados por el órgano jurisdiccional remitente en el marco del procedimiento principal, dicho órgano jurisdiccional alberga dudas acerca de si el Derecho de los Estados*

> *Unidos garantiza efectivamente el nivel de protección adecuado exigido en el artículo 45 del RGPD, interpretado a la luz de los derechos fundamentales garantizados en los artículos 7, 8 y 47 de la Carta. En particular, el referido órgano jurisdiccional considera que el Derecho de ese país tercero no prevé las limitaciones y las garantías necesarias con respecto a las injerencias autorizadas por su normativa nacional y tampoco garantiza una tutela judicial efectiva contra tales injerencias. En relación con este último aspecto, añade que la creación del Defensor del Pueblo en el ámbito del Escudo de la Privacidad no puede, a su entender, subsanar esas lagunas, ya que ese Defensor del Pueblo no puede asimilarse a un tribunal, en el sentido del artículo 47 de la Carta"* FJ 1.

La jurisprudencia de los Tribunales Españoles, en el ámbito de la protección de datos arranca con la sentencia del **Tribunal Constitucional** 110/1984, al considerar que, en el ámbito de actuación de la Dirección General de Inspección Financiera y Tributaria, se vulneraba el derecho a la intimidad FJ 6.

Una segunda sentencia del alto Tribunal, la STC 254/1993 considera que una decisión judicial vulnera el derecho a la intimidad, y no era ajustada a derecho sino permitía acceder a la información de datos personales existentes en ficheros automatizados de la Administración del Estado FJ 1 y FJ 7.

Supone la consolidación y definición del derecho a la protección de datos la sentencia, STC 290/2000 de 30 de noviembre, en relación con el conflicto de los preceptos impugnados de la LORTAD y las competencias atribuidas a las Comunidades Autónomas. Por ello por lo que el Tribunal Constitucional, en cuanto a la naturaleza y competencias de la Agencia de Protección de Datos, establece de forma clara que la garantía a los derechos, así como la igualdad de todos los españoles es el objetivo que guía, todas las actuaciones de la Agencia de Protección de datos, cualquiera que sea el territorio nacional dónde se encuentren los ficheros y sea quien sea el responsable de los mismos FJ 6 y FJ 7.

En este mismo sentido, la STC 292/2000, del 30 de noviembre, aporta pronunciamientos, a consecuencia de los recursos promovidos por el Defensor del Pueblo contra los artículos 21.1 y 24.1 de la Ley orgánica 15/1999. La importancia de esta sentencia radica, al enunciar que "*El derecho fundamental a la Protección de datos persigue garantizar a esa persona el poder de control sobre sus datos personales, sobre su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y derecho del afectado*.

> …*El objeto de protección del derecho fundamental a la protección de datos no se reduce solo, a los datos íntimos de la persona, sino a cualquier tipo de dato personal, sea íntimo o no, porque su objeto no es solo la intimidad individual, protegida por el artículo 18.1 de la CE, sino los datos de carácter personal"* FJ 6.

El alto Tribunal establece de forma definitiva, la diferencia entre el derecho a la intimidad y el derecho a la protección de datos. Siendo que el derecho a la intimidad impone un

deber de no intromisión en la esfera íntima de las personas y el derecho a la protección de datos les confiere a su titular facultades cuyo ejercicio impone a terceros deberes jurídicos, tales como el derecho a saber y ser informado sobre el destino y uso de los datos, el derecho a acceder, rectificar y cancelar los datos.

II

Brechas de Seguridad.

En contestación a la pregunta formulada por el cliente, en relación así la evaluación del riesgo y la notificación de la brecha se ha realizado correctamente, y por lo tanto si se ha cumplido con la normativa de protección de datos, corresponde en primer lugar, como elemento clave de la política de seguridad de datos, definir que es una Brecha de Seguridad.

Una brecha de seguridad es un incidente de seguridad que afecta a datos de carácter personal, independientemente de si la causa del incidente es un accidente, o una acción intencionada y sin que sea relevante que afecte a datos digitales, o a datos en formato papel, además provocan la destrucción, pérdida, alteración, comunicación o acceso no autorizado de datos personales.

Así mismo el RGPD, define a la brecha de seguridad, a las que llama violación de la seguridad de los datos personales, en el apartado 12 del artículo 4 dedicado a las definiciones, como sigue:

> *…" 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;"*

Las formas en las que se pueden producir las brechas de seguridad son infinitas, pero las especialmente frecuentes, son las que suceden en el entorno digital y van desde una modificación no autorizada de la base de datos, la destrucción de copias de seguridad, hasta ciber fraudes, como el caso que nos ocupa, dónde podemos observar diferentes resultados tales como la estafa informática, la usurpación de identidad o la filtración de correos electrónico, producido por el acceso no autorizado, con el fin de obtener una ventaja. Las organizaciones deben intentar evitarlas y en caso de que sucedan gestionarlas adecuadamente.

El citado Reglamento General de Protección de Datos, introduce un cambio importante en esta materia, ya que sitúa a las empresas cómo un elemento clave, esperando que cumplan de forma anticipada con el principio de proactividad, implementando medidas de seguridad adecuadas para evitar la materialización de incidentes de seguridad, y sean capaces, además, de reaccionar de una manera oportuna, si se materializa.

En este sentido el artículo 32, RGPD, sobre la Seguridad del Tratamiento, en el Capítulo 4º, sobre el responsable de Tratamiento y Encargado de tratamiento, en concreto en la Sección 2 de la Seguridad de los Datos Personales, se refiere a que los responsables y encargados aplicaran medidas técnicas y organizativas adecuadas al nivel de riesgo que comportan los tratamientos de datos que realizan, con la finalidad de garantizar un nivel de seguridad adecuado.

Las pautas para la gestión y notificación de las Brechas de Seguridad se ofrecen en el artículo 33 del mismo cuerpo legal, siendo posible facilitar la información de forma gradual.

Se ordena:

> "*1. En caso de violación de la seguridad de los datos personales, el responsable del tratamiento la notificará a la autoridad de control competente de conformidad con el artículo 55 sin dilación indebida y, de ser posible, a más tardar 72 horas después de que haya tenido constancia de ella, a menos que sea improbable que dicha violación de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas".*
>
> *3. La notificación contemplada en el apartado 1 deberá, como mínimo:*
>
> *a) describir la naturaleza de la violación de la seguridad de los datos personales, inclusive, cuando sea posible, las categorías y el número aproximado de interesados afectados, y las categorías y el número aproximado de registros de datos personales afectados;*
>
> *b) comunicar el nombre y los datos de contacto del delegado de protección de datos o de otro punto de contacto en el que pueda obtenerse más información;*
>
> *c) describir las posibles consecuencias de la violación de la seguridad de los datos personales;*
>
> *d) describir las medidas adoptadas o propuestas por el responsable del tratamiento para poner remedio a la violación de la seguridad de los datos*

personales, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos."

La previsión del artículo 34 del Reglamento citado, se refiere a la obligación del responsable del Tratamiento de realizar además una comunicación a los sujetos afectados, si supone un alto riesgo para los derechos y libertades de las personas físicas.

La Ley Orgánica de Protección de Datos y de Garantías de Derechos Digitales 3/2018 de, 5 de diciembre, establece en el artículo 72, dentro del Título IX referido al régimen sancionador, que el incumplimiento de las obligaciones que se derivan del RGPD sobre las brechas de seguridad, es considerada una infracción muy grave.

También se prevé, la **Ley 9/2014 de, 9 de mayo, Ley General de Telecomunicaciones**, en su artículo 41, cuando establece la obligación de informar sobre las brechas de seguridad que puedan comprometer datos personales a los operadores de servicios de comunicaciones electrónicas disponibles al público, a pesar de no ser una regulación específica del ámbito de la protección de datos.

Las disposiciones legales citadas plantean, de forma clara, el procedimiento que se ha de seguir, y en este sentido el responsable debe notificar el incidente a la Autoridad de protección de datos competente, a menos que sea improbable que la violación suponga un riesgo para los derechos y libertades de los afectados.

El Grupo de Trabajo del artículo 29, creado por la Directiva 95/46/CE, y sustituido desde el, 25 de mayo de 2018, por Consejo Europeo de Protección de Datos (EDPB) era un órgano consultivo independiente integrado por las Autoridades de Protección de Datos de todos los Estados miembros.
En orden a sus atribuciones, en su documento Directrices sobre la notificación de las violaciones de la seguridad de los datos personales, de acuerdo con el Reglamento 2016/679, adoptadas el, 3 de octubre de 2017, y revisadas por última vez el, 6 de febrero de 2018, (18/ES WP250 rev.01), explica los requisitos de la obligación

de notificación de las violaciones del RGPD en base al citado artículo 33, también a determinar en base a tres principios de la seguridad de la información.

Si la violación es de la confidencialidad, dado que se produce una revelación no autorizada o accidental de los datos personales, o bien la violación es en relación a la integridad, porque se produce una alteración no autorizada o accidental de los datos personales o por último una violación de la disponibilidad si se produce una pérdida de acceso accidental o no autorizada a los datos personales.

En relación a cuando es necesario notificar, precisa los mandatos del articulo 33 RGPD, y da luz sobre que significa, que la notificación se iniciara, cuando se tenga constancia, interpretando que se debe tener un grado razonable de certeza de que se ha producido un suceso, que compromete datos personales y puntualiza que en algunos casos será relativamente fácil determinarlo y que en otros puede llevar más tiempo establecerlo, pero en todo caso el Grupo hace hincapié en la celeridad de las actuaciones.

También se manifiesta sobre el concepto de notificación sin dilación indebida, fijando que con ello se hace referencia a que el plazo de las 72 horas da margen para realizar algunas investigaciones para reunir pruebas, después de la alerta inicial y la sospecha que se ha producido un incidente de seguridad que pueda afectar a datos personales para que se produzca la notificación y solo en casos excepcionales debe tardarse más tiempo.

El objetivo del requisito de notificación es alentar a los responsables del tratamiento a que actúen con prontitud en caso de violación, contenerla y, si es posible, recuperar los datos personales comprometidos.
El hecho de notificar a la autoridad de control dentro de las primeras setenta y dos horas puede permitir que el responsable del tratamiento se asegure de que las decisiones sobre si debe o no notificar a las personas sean correcta.

Si esta no se produce, se deberán indicar los motivos de la dilación, puesto que es posible que la notificación sea gradual, pero también ampara en base al artículo 33 RGPD que pueda permitirse una notificación con retraso, aunque esto no debería considerarse como algo que deba ocurrir con regularidad.

Por último, el Grupo considera que la referencia del articulo 33 RGPD sobre que no será necesario notificar cuando sea improbable que la brecha ..." *constituya un riesgo para los derechos y las libertades de las personas físicas" supone* tener en cuenta si los datos personales ya están disponibles al público y su comunicación no constituye un riesgo probable para la persona si se han hecho esencialmente ininteligibles.

Respecto al artículo 34 del RGPD las directrices sobre la comunicación al interesado, el Grupo del articulo 29 recomienda sobre los medios para comunicar a los afectados, que sea de forma separada y sin que coincida con otras informaciones para que la información sea clara y transparente y que se elijan un medio que aumente al máximo la posibilidad de comunicar a todas las personas afectadas de forma adecuada, apuntando incluso el uso de varios canales de contacto.

La Agencia Española de Protección de Datos se ha manifestado, en relación con la gestión y comunicación de las Brechas de Seguridad mediante la instrucción de un procedimiento donde de forma sistemática se pondera la cronología de los hechos, las causas que hicieron posibles la brecha de seguridad, los posibles eventos análogos en el tiempo, los datos afectados y las acciones tomadas para minimizar la brecha y las medidas de seguridad implantadas.

En concreto y a requerimiento de la pregunta relacionada con el cumplimiento de la normativa de protección de datos, en cuanto a la tramitación y notificación de la brecha, y a la vista del relato de los antecedentes de hecho, cabe manifestar que para poder acreditar que las actuaciones han sido acordes con los pedimentos legales, el procedimiento sistemático debe arrancar con un análisis inicial, para saber que ha pasado, definir el problema y valorar los aspectos relacionados con la gravedad y el origen de la misma.

Siendo probable que no se cuenten con todos los elementos de juicio se debe, realizar la notificación a las autoridades de control sin dilación indebida y a ser posible, dentro de las 72 horas siguientes a que el responsable tenga constancia de ella. Y, si dentro de este plazo, no se cuenta con toda la información, es posible realizar una notificación inicial para no incumplir el plazo señalado y aportar el resto de información a medida que se va conociendo.

Lo que subyace a dicha obligación de notificación, es un deber más amplio y que insta al responsable a implementar un procedimiento de gestión de incidentes de seguridad que afecten a datos de carácter personal adaptado a las características del tratamiento.

De la relación de hechos causales, se desprende que la entidad contaba con un protocolo interno de protección de datos, aunque en la práctica no se constata que se haya seguido, por la falta de sistemática que se desprende de sus actuaciones y porque las consecuencias sólo se miden en términos económicos.

La evaluación del riesgo del incidente no puede ser fruto de un conjunto de impresiones “personales”, bien al contrario, el parámetro determinante para notificar una brecha de datos personales a la Autoridad de Control o comunicarla a los afectados es el nivel de riesgo. No cualquier tipo de riesgo o un riesgo para la organización, sino específicamente el riesgo para los derechos y libertades de las personas físicas afectadas por la brecha.

Los criterios señalados por la Agencia Española de Protección de Datos pueden servir de orientación, para determinar el riesgo inherente al incidente y la necesidad de notificación, de modo que los parámetros a medir son **el volumen en número de registros** que se han visto afectados, **la tipología de los datos**, y **el impacto**, entendido como el grado de exposición que ha conllevado la brecha. A cada tramo se le asigna una magnitud de cálculo propuesta por la AEPD.

De este modo, el cálculo del posible riesgo se obtiene de la operación de multiplicar el valor asignado al volumen, por el resultado de la multiplicación de los valores de la tipología y el impacto y de este modo conocer, si debe ser notificada a la autoridad y si es recomendable también hacerlo a los interesados.

Esta actividad necesaria para la determinación de la necesidad, no se acredita en el relato de los hechos, solo meras suposiciones e impresiones personales, llevan a determinar que la brecha tiene poca importancia y cuando se descubren nuevas certezas sobre el alcance real, tampoco se evalúa el riesgo.

Las circunstancias fácticas hacen que las personas encargadas, ocupadas en las indagaciones, acuerden que lo mejor es ignorar la obligación de la notificación establecida por la normativa que, incluso ofrece cobertura para que la misma pueda ser extemporánea siempre que se acompañe de los motivos que ha propiciado rebasar el plazo.

Caber añadir que el proceso para la notificación es un proceso que puede realizarse de forma telemática, a través de los recursos que ofrece en su web la propia Autoridad de Control, que además ha editado una guía para proporcionar a los responsables, directrices generales en la notificación de brechas de datos personales y en la comunicación a los interesados, precisando plazos y aspectos concretos, sobre el procedimiento de notificación y el contenido de la misma. La información que proporciona permite al responsable conocer con precisión el alcance de sus obligaciones y facilitar su cumplimiento.

A la vista de todo lo expuesto hasta ahora, debemos concluir que las actuaciones llevadas a cabo por la farmacéutica, no se ajustan a los requerimientos legales establecidos en el artículo 33 RGPD, dado que se ha incumplido con la obligación de notificación a la Agencia Española de Protección de Datos.

No se analiza los supuestos riesgos para los derechos y libertades de los posibles afectados, se toma la decisión errónea de no realizar ninguna acción al respecto, con clara infracción al artículo 34, del mismo cuerpo legal.

No hay focalización de los esfuerzos, en evitar y mitigar las posibles consecuencias desfavorables para los afectados y en ningún caso se ha conseguido la protección efectiva de los derechos y libertades públicas de las personas afectadas.

III

Delegado de Protección de Datos

Por lo que se refiere a la cuestión planteada, sobre si el delegado de protección de datos de la entidad ha llevado a cabo sus responsabilidades correctamente, advertiremos en primer lugar, que los laboratorios usan la denominación de responsable y delegado de protección de datos indistintamente, sin advertir que ello les induce al error de pensar que cuentan con la figura del delegado de Protección de Datos, regulada en el RGPD, y se solicita saber si ha actuado correctamente.

Cabe destacar en primer lugar, que esta figura es una novedad y constituye uno de los elementos claves del Reglamento General de Protección de Datos, como garante del cumplimiento de la normativa de protección de datos en las organizaciones, sin sustituir las funciones que desarrollan las Autoridades de Control.

En virtud del RGPD, es obligatorio que algunos responsables y encargados del tratamiento designen un DPD. Así será en el caso de todas las autoridades y organismos públicos (con independencia de qué datos traten), y de otras organizaciones cuya actividad fundamental consista en la observación sistemática de personas a gran escala, o que traten categorías especiales de datos personales a gran escala.

Esta figura, desarrollada en los artículos 37, 38 y 39 del Reglamento UE 2016/679, supone haber realizado un nombramiento formal, y la obligación de ser comunicado a la autoridad de control pertinente. Los citados artículos se refieren a la designación, a la posición que ocupa en la organización y a sus funciones.

El Grupo del artículo 29, adoptó unas Directrices sobre el DPD en fecha, 13 de diciembre de 2016, revisadas por última vez y adoptadas el 5 de abril de 2017 y se manifiesta sobre el nombramiento obligatorio, pero también valora que se pueda nombrar de forma voluntaria y establece para este caso, que deberá seguir los mismos requerimientos que ofrecen los artículos 37, 38, 39 del citado cuerpo legal.

La Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantías de los Derechos Digitales, se regula en el Capítulo III, la figura del delegado de Protección de Datos. En concreto, el artículo 34 lo hace en los mismos términos que el artículo 37.1 del Reglamento, en cuanto a su designación y aporta un listado de entidades que tienen la obligación de realizar el nombramiento, allanando el camino sobre la obligatoriedad del nombramiento de esta figura.

En el apartado segundo del mismo artículo 34, se reconoce la posibilidad de un nombramiento voluntario, quedando sometido al mismo régimen establecido para el caso de ser obligatorio.

El papel que juega el DPD en la entidad que la nombra, aparecen recogidas en el artículo 39 del Reglamento, el cual ofrece una enumeración de las funciones que se le asignan, debe informar y asesorar a la organización en la materia y supervisar el cumplimiento de lo dispuesto en el citado Reglamento y otras disposiciones de aplicación.

Su papel es de apoyo y ayuda ante cualquier eventualidad o problema que pueda surgir en relación con la aplicación de los preceptos reglamentarios, pero no se le

asigna un papel especialmente activo en la gestión y notificación de la brecha, tal como se dispone para la Evaluación de Impacto del artículo 39. 1. C del citado Reglamento o la intervención del DPD en caso de reclamación ante las autoridades de protección de datos, descrito en el artículo 37 de la ya citada ley 3/2018 LOPDGDD.

En todo caso, de facto el DPD ocupará un papel muy relevante en el proceso de gestión de brechas. El Reglamento General de Protección de datos, encomienda al delegado de Protección de Datos, la función de informar y asesorar al responsable o encargado de las obligaciones que les incumben, incluidas las relativas a la gestión y notificación de las brechas de datos personales, así como cooperar con la Autoridad de Control y actuar como punto de contacto con la misma para cuestiones relativas al tratamiento.

En este sentido, su asesoramiento ira dirigido a la implantación de un proceso de gestión de brechas de datos personales en la organización, a la evaluación del riesgo y las consecuencias que puede suponer para los derechos y libertades de las personas una brecha de datos personales, a las acciones adecuadas que se deben tomar para mitigar los efectos de la brecha de Datos Personales sobre las personas afectadas, a la necesidad de notificar la brecha de Datos Personales a la Autoridad de Control y en su caso a los interesados afectados.

Para el desarrollo de sus funciones, deberá contar con los medios y la información necesarios. No obstante, la responsabilidad recae ineludiblemente en el responsable del tratamiento respecto de sus obligaciones.

Advertimos que la confusión entre responsable y delegado, entendida por la entidad como la persona que gestiona los temas relacionados con la protección de datos, ha llevado a solicitar el pronunciamiento, pero en este ámbito, los diferentes intervinientes en la gestión de la brecha, siendo que no ocupan la posición de delegado de Protección de Datos previstos en la normativa, no podemos entrar a valorar actuaciones de dichas personas, bajo los pedimentos exigidos legalmente.

La redacción del presente informe nos ofrece la posibilidad de poner en valor la necesidad de que la organización se plantee el nombramiento formal y expreso de un delegado de Protección de Datos, que a la vista de todo lo expuesto, hubiera supuesto tener al frente de la gestión del incidente, a un profesional con conocimientos en Derecho y en especial en materia de Protección de Datos.

IV

Delitos informáticos.

El uso de las nuevas tecnologías conlleva indudables ventajas, pero también sirve de cauce para la aparición de conductas, que además de suponer infracción a la normativa de protección de datos desemboca en la comisión de delitos, que se manifiestan tanto en conductas donde la informática es el objeto del delito como en conductas donde los sistemas informáticos son el medio para cometer el delito.

La decisión Marco del Consejo de ministros de la Unión europea de, 28 de mayo del 2001, dispone que los Estados Miembros deberán de adoptar medidas necesarias, para garantizar que sean delitos penales cuando se produzcan de forma deliberada la realización o provocación de transferencias de dinero u otros valores, mediante mecanismos que supongan alteración, borrado o supresión indebida de datos informáticos, especialmente datos de identidad, tal como plantea el artículo 3 de la citada decisión, cuyo tenor literal:

> "*Delitos relacionados con equipos informáticos*
>
> *Cada Estado miembro adoptará las medidas necesarias para garantizar que las siguientes conductas sean delitos penales cuando se produzcan de forma deliberada:*
>
> *realización o provocación de una transferencia de dinero o de valor monetario que cause una pérdida no autorizada de propiedad a otra*

persona, con el ánimo de procurar un beneficio económico no autorizado a la persona que comete el delito o a terceros, mediante:
- la introducción, alteración, borrado o supresiones indebidas de datos informáticos, especialmente datos de identidad, o
- la interferencia indebida en el funcionamiento de un programa o sistema informática."

El fraude como ilícito en el derecho penal español, engloba una serie de conductas encaminadas a llevar al engaño a las víctimas y que comporta realizar un acto de disposición en su perjuicio, tal y como establece el artículo 248.1 del CP.

1. *"Cometen estafa los que, con ánimo de lucro, utilizaren engaño bastante para producir error en otro, induciéndolo a realizar un acto de disposición en perjuicio propio o ajeno".*

La estafa es un delito patrimonial en el que, a través del engaño suficiente, y concurriendo ánimo de lucro, se provoca un error esencial en la víctima que le lleva a realizar un acto de disposición patrimonial en perjuicio de ella misma o de un tercero.

El bien jurídico protegido en todas las modalidades de estafa es el patrimonio ajeno y el daño patrimonial debe ser susceptible de valoración económica. Así, en el delito de estafa, el tipo subjetivo exige la apreciación de dolo defraudatorio y de ánimo de lucro y, consecuentemente, se generará un perjuicio hacia la víctima que ha sufrido la estafa.

La reforma introducida por la **Ley Orgánica 10/1995 de, 23 de noviembre**, añade al mencionado artículo 248 del CP un apartado segundo, que se expresa en los siguientes términos y que mantiene la redacción siguiente:

2." *También se consideran reos de estafa: a) Los que, con ánimo de lucro y valiéndose de alguna <u>manipulación informática</u> o artificio semejante,*

consigan una transferencia no consentida de cualquier activo patrimonial en perjuicio de otro".

La modalidad de estafa mediante manipulación informática se trata de un tipo que no presenta la misma dinámica que la estafa tradicional, ya que la finalidad es recoger conductas lesivas al patrimonio ajeno, sin que la piedra angular sea el engaño.

Teniendo en cuenta los requisitos que se exige en el delito de estafa como tipo básico, mencionados anteriormente, en la estafa informática también ha de apreciarse, ánimo de lucro, un acto de disposición patrimonial en perjuicio de un tercero y una defraudación.

El engaño, como conducta típica, presenta singularidades en el tipo penal del delito de estafa informática. Como elemento propio de las relaciones personales, en este tipo, el engaño no se distingue como tal, puesto que actúan otros sujetos sin personalidad, pero que son el medio para cometer el acto delictivo, se trata de máquinas o sistemas informáticos y ello complica su acreditación para poder ser denunciado.

En estos casos, el engaño se sustituye con la manipulación informática, dado que la máquina o sistema informático, actúa por orden de una conducta ilegitima, que modifica elementos físicos o introduce datos falsos y dichos elementos actúan conforme se las programe y detrás de todo ello, se encuentra el verdadero artífice y beneficiario patrimonial.

En este sentido, el concepto de manipulación informática que introduce el Código Penal es suficientemente amplio como para tener cabida, desde un punto de vista técnico, cualquier tipo de manipulación que presenta capacidad para lesionar el patrimonio ajeno.

La STS 533/2007 de, 12 de junio, fundamenta que "*no es precisa la concurrencia de engaño alguno por el estafador, porque el acecho a patrimonios ajenos realizados*

mediante manipulaciones informáticas actúa con automatismo en perjuicio de terceros, precisamente porque existe la manipulación informática y por ello no existe el engaño personal" FJ 2.

En este mismo sentido, se manifiesta la STC 860/08 de, 17 de diciembre de 2008, al avalar la tipicidad del artículo 248.2 para las estafas informáticas, en el sentido siguiente: " *Cuando la conducta que desapodera a otro de forma no consentida de su patrimonio se realiza mediante manipulación del sistema informático, bien del equipo, bien del programa, se incurre en la tipicidad del art. 248.2 del CP. También cuando se emplea un artificio semejante. Una de las acepciones del término artificio hace que este signifique artimaña, doblez, enredo o truco*" FJ 2.

Como dice la STS 603/2000, de 20 de noviembre, *"La actual redacción del art. 248.2 del Código Penal permite incluir en la tipicidad de la estafa aquellos casos que mediante una manipulación informática o artificio semejante se efectúa una transferencia no consentida de activos en perjuicio de un tercero admitiendo diversas modalidades, bien mediante la creación de órdenes de pago o de transferencias, bien a través de manipulaciones de entrada o salida de datos, en virtud de los que la máquina actúa en su función mecánica propia"* FJ 3.

En concreto y a requerimiento de la pregunta si es conveniente emprender acciones penales, las operaciones que se describen en el relato fáctico de los hechos, constituyen delito de estafa informática, porque a través del acceso a datos de correos electrónicos, y mediante manipulación informática, sin concurrencia de engaño ni colaboración de las víctimas, se produce el desplazamiento patrimonial.

Las acciones se dirigen contra los sistemas informáticos, que facilitan el acceso a las cuentas bancarias legítimas y la realización de disposiciones económicas, mediante transferencias bancarias, apreciándose ánimo de lucro, actos de disposición patrimonial en perjuicio de terceros y una defraudación.

La forma más aconsejable de iniciar las acciones es mediante la presentación de una denuncia ante las Fuerzas y Cuerpos de Seguridad del Estado, puesto que se requerirá una investigación por parte de los mismos, que prestaran especial atención a los hechos en concreto, para poder recopilar pruebas inculpatorias.

En la denuncia no será necesario determinar al responsable de los hechos, aunque si se tuviera una sospecha, es aconsejable hacerlo constar, para que la investigación pueda dirigirse en ese sentido.

Es conveniente poner en conocimiento de las farmacias implicadas, que la compañía se personará en las causas que se sigan en relación con la materialización del delito de estafa en sus negocios, concretado en la redacción de los antecedentes de hecho del presente informe.

CONCLUSIONES

Brecha de Seguridad.

La empresa TURBOFARMA COMPLET, S.L., no se ajusta a los requerimientos legales establecidos en el artículo 33 del RGPD, dado que ha incumplido con la obligación de notificación a la Agencia Española de Protección de Datos. El plazo establecido de 72 horas ha de ser observado sin dilación indebida.

El responsable puede autorizar a una persona física, representante o entidad que ejerza su representación para que realice la notificación de la brecha de datos personales ante la Autoridad de Control.

Es recomendable realizar una notificación inicial, dentro del plazo establecido y con posterioridad y de forma gradual facilitar el resto de información requerida.

No se han observado esfuerzos para evitar y mitigar las posibles consecuencias desfavorables para los afectados y en ningún caso se ha conseguido la protección efectiva de los Derechos y Libertades públicas de las personas afectadas.

Delegado de Protección de Datos.

En cuanto al delegado de Protección de Datos, no consta su nombramiento, expreso para cumplir estrictamente con el requerimiento legal establecido al efecto, lo que nos lleva a concluir que está figura no está implantada en la compañía.

Se advierte a la empresa de la confusión que existe en el seno de su organización, al creer erróneamente que cualquier persona, que de forma interna se encargue de los asuntos relacionados con la protección de datos, adquiere el rol de delegado de Protección de Datos según lo establecido en el RGPD.

El DPD es una figura clave a partir del Reglamento, es el garante del cumplimiento de la normativa en las organizaciones. Se trata de un profesional que deberá contar con conocimientos especializados del Derecho y singularmente en materia de protección de datos.

Delito Informático.

Por lo que hace referencia el delito informático, es conveniente que la mercantil TURBOFARMA COMPLET, S.L. emprenda acciones penales, puesto que, queda totalmente demostrado que las acciones se dirigen contra los sistemas informáticos, que facilitan el acceso a las cuentas bancarias apreciándose ánimo de lucro.

Se produce desplazamiento patrimonial, porque a través del acceso a datos de correos electrónicos y mediante manipulación informática, sin concurrencia de engaño ni colaboración alguna de las víctimas se materializan las estafas.

En relación con las farmacias clientes que se han visto afectadas, es recomendable personarse en las causas, porque a pesar de no tratarse de un derecho propio, la compañía ha de tener interés en evitar los efectos reflejos de las sentencias que se dicten en su momento.

Este es el Informe que emito según mi leal saber y entender, y que someto a cualquier otro mejor fundamento en Derecho.

ANEXO A: BIBLIOGRAFÍA DEL TFG

- COTINO HUESO, Lorenzo, Encuesta sobre la Protección de Datos, UNED, *Teoría y Realidad Constitucional,* número 46 (2020), página 70-71.

- GARCÍA MAHAMUT, Rosario, Encuesta sobre la Protección de Datos, UNED, *Teoría y Realidad Constitucional,* número 46 (2020), página 71 - 73.

- LUCAS MURILLO DE LA CUEVA, Pablo, Encuesta sobre la Protección de Datos, UNED, *Teoría y Realidad Constitucional,* número 46 (2020), página 74 - 75.

- MEDINA GUERRERO, Manuel, Encuesta sobre la Protección de Datos, UNED, *Teoría y Realidad Constitucional,* número 46 (2020), página 75.

- QUINTERO OLIVARES, Gonzalo, " Comentario al artículo 248", Libro II: Título XIII *Comentarios a la parte especial del Derecho Penal,* Editorial Aranzadi en Cizur Menor, (2002), página 668 - 678.

- RALLO LOMBARTE, Artemi, Encuesta sobre la Protección de Datos, UNED, *Teoría y Realidad Constitucional,* número 46 (2020), página 75 - 78.

- REBOLLO DELGADO, Lucrecio, Encuesta sobre la Protección de Datos, UNED, *Teoría y Realidad Constitucional,* número 46 (2020), página 78 - 80.

- TRONCOSO REIGADA, Antonio, Encuesta sobre la Protección de Datos, UNED, *Teoría y Realidad Constitucional,* número 46 (2020), página 80 - 85.

- VIDAL FUEYO, Camino, Encuesta sobre la Protección de Datos, UNED, *Teoría y Realidad Constitucional,* número 46 (2020), página 85 - 87.

ANEXO B: WEBGRAFÍA DEL TFG

- Agencia Española de Protección de Datos (AEPD), Derechos y Deberes: https://www.aepd.es/es/derechos-y-deberes/cumple-tus-deberes/medidas-de-cumplimiento/brechas-de-, 20-11-2020.

- Agencia Española de Protección de Datos (AEPD), Brechas de seguridad: https://www.aepd.es/es/prensa-y-comunicacion/blog/brechas-de-seguridad-de-datos-personales-que-son-y-como-actuar, 22-11-2020.

-Agencia Española de Protección de Datos (AEPD), Guía Brechas de Seguridad: https://www.aepd.es/sites/default/files/2019-09/guia-brechas-seguridad.pdf, 22-11-2020.

-Grupo ático 34 (consultoría empresarial), como se notifican las brechas de seguridad: https://protecciondatos-lopd.com/empresas/notificar-brechas-seguridad/,12-12-2020.

-Grupo ático 34 (empresa en consultoría empresarial), suplantación de identidad: https://protecciondatos-lopd.com/empresas/suplantacion-de-identidad/, 12-12-2020.

- Perito Judicial Group, delito y denuncia de la suplantación de identidad: https://peritojudicial.com/suplantacion-de-indentidad-denunciar/, 10-01-2021.

-ACEN (Empresa especialista en protección de datos), La importancia de cumplir con la protección de datos: http://www.acennavarra.com/la-importancia-de-cumplir-con-la-ley-de-proteccion-de-datos/, 20-01-2021.

- Protección Data, (Empresa especializada en protección de datos y compliance), orígenes de la normativa: https://protecciondata.es/un-poco-de-historia-los-origenes-de-la-actual-normativa/, 14-05-2021.

-Agencia Estatal Boletín Oficial del Estado, Ley 9/ 2014 de 9 de mayo General de Telecomunicaciones:https://www.supercontable.com/informacion/ley_gestion/Articulo_41.Ley_9-2014-_de_9_de_mayo-_General_.html, 14-05-2021.

-V/ lex España información jurídica inteligente, consulta de la STS 860/2008, de 17 diciembre de 2008: https://supremo.vlex.es/vid/1-6-52049423, 16-05-2021.

-Noticias Jurídicas, estafa informática normativa: https://noticias.juridicas.com/conocimiento/artículos-doctrinales/10617-estada-informática-el-denominado-, 16-05-2021.

-Iberley, Concurso de delitos juntamente con la estafa informática: https://www.iberley.es/temas/concurso-delitos-estafa-informatica-65367, 16-05-2021.

ANEXO C: NORMATIVA APLICABLE AL TFG.

-Convenio Europeo de los Derechos Humanos del 4 de noviembre de 1950.

- Convenio N.º 108 del Consejo de Europa, de 28 de enero de 1981.

-Tratado de funcionamiento de la Unión Europea, firmado en Roma.

-El Reglamento UE 2016/679, del Parlamento Europeo y del Consejo del, 27 de abril del 2016.

-Reglamento UE 2018/1807 del Parlamento Europeo y del Consejo de, 14 de noviembre de 2018, relativo a un marco para la libre circulación de datos no personales en la Unión Europea.

-Directiva 95/46 CE, relativa a la Protección de Datos de las personas físicas, del Parlamento Europeo y el Consejo en fecha, 24 de octubre de 1995.

-Directiva (UE) 2016/680, del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo.

-Ley Orgánica 15/1999 del, 13 de diciembre, de Protección de Datos de carácter personal, (LOPD). Entro en vigor el, 14 de enero del año 2000.

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

-Ley Orgánica 5/1992 de, 29 de octubre, de Regulación del Tratamiento Automatizado de Datos de Carácter Personal (LORTAD).

- Ley Orgánica 10/1995 de, 23 de noviembre.

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

-Ley 9/2014, de 9 de mayo, General de Telecomunicaciones.

ANEXO D: JURISPRUDENCIA.

TJUE→ e- curia, https://curia.europa.eu/jcms/jcms/P_78957/es/

- Sentencia del Tribunal de Justicia de la Unión Europea C- 131/12, de 13 de mayo.

TJUE→ e- curia, https://curia.europa.eu/jcms/jcms/P_78957/es/

- Sentencia del Tribunal de Justicia de la Unión Europea C- 311/18, de 16 de julio.

TC→ https://www.tribunalconstitucional.es/es/jurisprudencia/Paginas/default.aspx

-Sentencia del Tribunal Constitucional 110/1984, de 21 de diciembre.

TC→ https://www.tribunalconstitucional.es/es/jurisprudencia/Paginas/default.aspx

-Sentencia del Tribunal Constitucional 254/1993, de 18 de agosto.

TC→ https://www.tribunalconstitucional.es/es/jurisprudencia/Paginas/default.aspx

- Sentencia del Tribunal Constitucional 290/ 2000, de 30 de noviembre.

TC→ https://www.tribunalconstitucional.es/es/jurisprudencia/Paginas/default.aspx

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

TS→ Poder Judicial de España, https://www.poderjudicial.es/cgpj

- Sentencia del Tribunal Supremo 533/ 2007, de 12 de junio.

TS→ Poder Judicial de España, https://www.poderjudicial.es/cgpj

- Sentencia del Tribunal Supremo 860/08, de 17 de diciembre.

TS→ Poder Judicial de España, https://www.poderjudicial.es/cgpj

- Sentencia del Tribunal Supremo 603/ 2000, de 20 de noviembre.