TFM-Aspectos legales de la seguridad informática

MISTIC 2012

Contenido

Objeto 3
Metodología 4
Supuesto I 5
Análisis previo 5
Estudio del caso 5
Estudio del caso desde el punto de vista del Hospital de Gerona 6
Estudio del caso desde el punto de vista de la empresa CIES 8
Conclusiones 10
Supuesto II 12
Introducción 12
Estudio del caso 12
Medidas de seguridad aplicadas por el Hospital 12
Valoración de la actuación del Hospital 14
Conclusiones 15
Supuesto III 17
Introducción 17
Estudio del caso 17
Estudio desde el punto de vista de la empresa 20
Estudio desde el punto de vista de Óscar 21
Conclusiones 22

Objeto

Este documento, junto a la presentación en PowerPoint adjunta, conforman el proyecto fin del máster MISTIC de la UOC.

Metodología

Para la realización del proyecto se ha seguido una metodología propia, con el fin de mantener un orden y coherencia entre los diferentes casos. Como paso inicial se realizó un estudio de la normativa vigente en materia de LOPD, estatuto de los trabajadores y la parte del Código Penal que afecta directamente al ámbito del proyecto.

La metodología empleada para el estudio de cada caso planteado ha seguido tres pasos fundamentales:

1. Estudio de los antecedentes del caso, como puede ser la situación laboral entre los implicados en el caso, hábitos o comportamientos en las situaciones que conforman el caso, etc. De esta fase se obtienen los imperativos legales que han de cumplir respecto a la LOPD.
2. Análisis pormenorizado de cada implicado en el caso. En esta fase se analiza cada implicado estudiando sus actuaciones, partiendo del estudio realizado en la fase anterior, y obteniendo implicaciones legales de los actos, faltas cometidas, o actuaciones correctas y dentro de la ley.
3. Estudio conjunto del caso y conclusiones, extrayendo las infracciones y sanciones derivadas de las actuaciones de los implicados.

A partir de esta información se ha elaborado el presente informe, estructurando cada supuesto en las siguientes partes:

- Análisis previo: en este apartado se analiza la información proporcionada en el supuesto, de forma objetiva, a modo de exposición inicial del caso. Se hace una primera valoración general de los hechos sin entrar a detallar las actuaciones de los implicados.
- Estudio del caso: en este apartado se exponen detalladamente las actuaciones de los implicados en el caso, cotejándolas con la legislación y normativa vigente a fin de detectar las posibles infracciones y faltas cometidas, o verificando en su caso que las actuaciones han sido correctas.

  En algunos casos se ha considerado interesante separar la información desde el punto de vista de cada implicado, para que su exposición fuese más clara.

- Conclusiones: en este apartado se exponen las conclusiones del caso, indicando quién ha obrado correctamente, quién ha incurrido en faltas, qué gravedad e infracciones suponen dichas faltas, etc. todo bajo el amparo y según dicta la ley vigente.

Supuesto I

Análisis previo

Para el análisis de este supuesto hay que tener en cuenta diversos aspectos, basándonos en la información proporcionada. Los más importantes serán determinar el **nivel de protección** que requieren los datos de pacientes que maneja el hospital y las **medidas de seguridad** que la ley exige para ellos. Con estos datos se podrá determinar si el hospital tenía implantadas estas medidas o si estaba incumpliendo alguna de ellas.

En este caso parece que puede haber un problema con la cesión de datos por parte del Hospital de Gerona a la empresa privada CIES. Hay que tener en cuenta que el hospital debe tener una serie de procedimientos que ha de cumplir, dada la cesión de datos, como pueden ser el avisar e informar adecuadamente a los pacientes de que se va a realizar este tratamiento con sus datos personales, estudiar el contrato de confidencialidad firmado con la empresa, etc.

Puede tener su relevancia también el hecho de que el estudio estadístico es una petición del Consorcio al Hospital, para que sea realizado por la empresa privada CISE. Habrá que analizar si pueden existir implicaciones legales a favor de la cesión en el hecho de que la petición provenga de una institución pública.

Con esta información se podrá deducir si el hospital ha incurrido en alguna infracción o delito, y estudiar las posibles sanciones derivadas de tal hecho.

Estudio del caso

Según el artículo. 3.A de la LOPD, use entiende por dato de carácter personal:

> [Art. 3.A LOPD] Datos de carácter personal: cualquier información concerniente a personas físicas identificadas o identificables.

Lo primero que es evidente es que los datos son de carácter personal ya que es información concerniente a personas físicas identificadas, ya que en la ficha del paciente siempre se incluyen nombres y apellidos y otro tipo de información identificativa.

Además en este caso, y según el artículo 7.3, son datos especialmente protegidos, al tratarse de datos concernientes a la salud de personas físicas:

> [Art. 7.3 LOPD] Los datos de carácter personal que hagan referencia al origen racial, a la salud y a la vida sexual sólo podrán ser recabados, tratados y cedidos cuando, por razones de interés general, así lo disponga una ley o el afectado consienta expresamente.

Según la LOPD, las **medidas de seguridad** que se deben adoptar para este tipo de datos especialmente protegidos engloban las medidas de nivel alto, medio y bajo. Por lo tanto el Hospital debería cumplir las siguientes condiciones:

- Debe existir un **responsable de seguridad** designado en el Hospital, encargado de controlar las medidas de seguridad aplicadas al fichero y los documentos.
- Debe contar con una relación detallada de los **usuarios** dados de alta en el sistema, controlando su **acceso** mediante mecanismos como contraseñas, que sean únicas y privadas, y se modifiquen periódicamente.
- Debe llevar un **registro de accesos** a los sistemas, que debe ser revisado periódicamente por el responsable de seguridad.
- En el sistema informático del Hospital debe contar con un **sistema de perfiles** claramente definido, de forma que se apliquen dichos perfiles al personal del Hospital según el trabajo que realicen y la información a la que tengan que acceder para realizar dicho trabajo.
- Si se emplean **redes inalámbricas**, deben estar protegidas y cifradas correctamente.
- El **acceso físico** a las instalaciones en las que haya información sensible debe estar controlado y restringido. En caso de almacenar información en formato físico, debe estar custodiada correctamente (por ejemplo, en ficheros bajo llave).
- **Formación** y **difusión** de la LOPD, obligaciones y responsabilidades de los empleados del Hospital al estar tratando información sensible de los pacientes.
- Debe contar con un sistema de registro de **incidencias** y notificación de las mismas.
- Debe contar con procedimientos de **backup** y restauración de la información.
- El **transporte y distribución** de los datos debe realizarse de forma cifrada.
- Debe proporcionar los mecanismos necesarios para que los pacientes ejerzan sus **derechos A.R.C.O**.
- Debe realizar **auditorías** al menos cada dos años, del estado de cumplimiento de la LOPD.

A continuación analizaremos los diferentes puntos de vista para comprobar si se cumplen estas medidas de seguridad, si la cesión de datos se realiza correctamente, etc.

Estudio del caso desde el punto de vista del Hospital de Gerona

Partimos del supuesto de que el Hospital ha dado de alta el fichero de los datos de sus pacientes en la Agencia. Estos ficheros de datos protegidos deben inscribirse en la Agencia de Protección de datos y además **informar a los afectados de la recogida** de los mismos y de la existencia del fichero así como su finalidad y sus derechos ARCO [Art. 5 LOPD].

> [Art. 5 LOPD]. Derecho de información en la recogida de datos.
>
> 1. Los interesados a los que se soliciten datos personales deberán ser previamente informados de modo expreso, preciso e inequívoco:

> a. De la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información.
>
> b. ...
>
> d. De la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición.

Segundo. El Hospital ha cedido un listado de datos de varios pacientes a la empresa CISE con el fin de que ésta realice una labor encargada por la Generalitat. Este listado no se encuentra disociado, es decir, se puede identificar a los pacientes cuyos datos figuran en él.

Al no encontrarse los datos disociados al enviarlos a la empresa CISE, en cuyo caso no habría problemas [Art 11.6 LOPD] ya que no se podría identificar al paciente, se da por hecho que dicha empresa podrá relacionar un historial clínico con un paciente concreto.

> [Art. 11.6 LOPD] Si la comunicación se efectúa previo procedimiento de disociación, no será aplicable lo establecido en los apartados anteriores.

Tercero. Según el principio de seguridad y confidencialidad del tratamiento de datos, el responsable del fichero (Hospital de Gerona) ha de salvaguardar la seguridad y confidencialidad adoptando medidas de seguridad y además está el deber de secreto profesional de los médicos respecto a los pacientes. Por lo tanto, los datos de salud de los pacientes deberían permanecer bien salvaguardados en todo momento.

Cuarto. Según el artículo 6.2 de la LOPD no se requiere consentimiento del afectado para recoger y tratar los datos cuando éstos se recojan para el ejercicio de las funciones propias de las Administraciones Públicas. Estamos suponiendo que el Hospital General de Gerona es un hospital público por lo tanto no necesitaría recoger el consentimiento.

> [Art. 6.2 LOPD] No será preciso el consentimiento cuando los datos de carácter personal se recojan para el ejercicio de las funciones propias de las Administraciones públicas en el ámbito de sus competencias; cuando se refieran a las partes de un contrato o precontrato de una relación negocial, laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento; cuando el tratamiento de los datos tenga por finalidad proteger un interés vital del interesado en los términos del artículo 7, apartado 6, de la presente Ley, o cuando los datos figuren en fuentes accesibles al público y su tratamiento sea necesario para la satisfacción del interés legítimo perseguido por el responsable del fichero o por el del tercero a quien se comuniquen los datos, siempre que no se vulneren los derechos y libertades fundamentales del interesado.

Y aunque no fuese hospital público, al tratarse de un hospital, **puede realizar el tratamiento** de los datos personales del afectado ya que es una *prestación sanitaria* y son tratados por personal sanitario que está sujeto al deber de secreto profesional, tal y como se refleja en los artículos 7.6 y 8 de la LOPD.

> [Art. 7.6 LOPD] No obstante lo dispuesto en los apartados anteriores, podrán ser objeto de tratamiento los datos de carácter personal a que se refieren los apartados 2 y 3 de este artículo, cuando dicho tratamiento resulte necesario para la prevención o para el **diagnóstico médicos, la prestación de asistencia sanitaria o tratamientos médicos o la gestión de servicios sanitarios**, siempre que dicho tratamiento de datos se realice por un profesional sanitario sujeto al secreto profesional o por otra persona sujeta asimismo a una obligación equivalente de secreto.

> [Art. 8 LOPD] Sin perjuicio de lo que se dispone en el artículo 11 respecto de la cesión, **las instituciones y los centros sanitarios públicos y privados y los profesionales correspondientes podrán proceder al tratamiento** de los datos de carácter personal relativos a la salud de las personas que a ellos acudan o hayan de ser tratados en los mismos, de acuerdo con lo dispuesto en la legislación estatal o autonómica sobre sanidad.

Por lo que el hecho de no pedir el consentimiento, si no se estuviera haciendo, no sería una falta o infracción.

El estudio del **cumplimiento de las medidas de seguridad** expuestas anteriormente queda fuera del ámbito de este proyecto, dado que es imposible verificar su estado con la información proporcionada en el enunciado del caso.

Se puede deducir, en todo caso, algunos hechos. Por ejemplo, es probable que el personal del Hospital no tenga la suficiente formación en materia de LOPD, ya que se ha dado este caso de cesión "ilícita". Habría que investigar por otra parte, si el traspaso de los datos a la empresa CIES se realizó en un formato cifrado, tal y como exige una de las medidas de seguridad de nivel alto para el transporte y distribución de la información.

Estudio del caso desde el punto de vista de la empresa CIES

En este caso **se trata de una cesión a terceros** y no de un acceso de los datos por parte de terceros ya que la empresa no está realizando un trabajo o servicio por cuenta del Hospital (el cual sería el responsable de los datos según la información proporcionada en la práctica). Lo hace por encargo y cuenta del Consorcio para la Normalización Lingüística.

En cuanto a la **cesión o comunicación** de los datos a un tercero, al tratarse de datos que **requieren un nivel alto de protección** (son datos especialmente protegidos), se requiere el

consentimiento del afectado, e informarle de la finalidad y actividad del tercero [Art. 11.1 LOPD].

> [Art. 11.1 LOPD] Los datos de carácter personal objeto del tratamiento sólo podrán ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del interesado.

Sólo podrán ser tratados por ese tercero con **fines** directamente relacionados con las funciones legítimas (en este caso sería realizar una estadística). Además habría que **informar** a los afectados de la primera cesión, la finalidad, naturaleza de los datos cedidos y el nombre y dirección del cesionario [Art. 27 LOPD].

> Art. 27 LOPD. Comunicación de la cesión de datos.
>
> 1. El responsable del fichero, en el momento en que se efectúe la primera cesión de datos, deberá informar de ello a los afectados, indicando, asimismo, la finalidad del fichero, la naturaleza de los datos que han sido cedidos y el nombre y dirección del cesionario.
>
> 2. La obligación establecida en el apartado anterior no existirá en el supuesto previsto en los apartados 2, letras c), d), e) y 6 del artículo 11, ni cuando la cesión venga impuesta por ley.

Existe una excepción [Art. 11.2.e LOPD] por la cual no se obligaría a recabar el consentimiento de los afectados y es que los datos se cedieran a un organismo público con fines estadísticos. Pero en este caso aunque la petición parte de un ente público como es la Generalitat, los datos se ceden realmente a una empresa privada, por lo que sí habría que recabar el consentimiento.

> [Art. 11.2e LOPD] Cuando la cesión se produzca entre Administraciones públicas y tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos.

El contrato o compromiso de confidencialidad que tiene el Hospital con la empresa no exime de tener que recoger el **consentimiento**, sino que es un "seguro" para que los datos cedidos no se utilicen para otra cosa que no sea el estudio estadístico y se adopten medidas de seguridad adecuadas en su tratamiento.

Asimismo habrá que tener en cuenta el deber de guardar secreto, establecido en el artículo 10 de la LOPD, ya que en este caso no se ha guardado (se han dado a conocer a un tercero los datos privados de varios pacientes).

> [Art. 10 LOPD] El responsable del fichero y quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal están

> obligados al secreto profesional respecto de los mismos y al deber de guardarlos, obligaciones que subsistirán aun después de finalizar sus relaciones con el titular del fichero o, en su caso, con el responsable del mismo.

Conclusiones

Tras la evaluación de los hechos se concluye que al tratarse de una cesión de datos a terceros, y ya que no se trata de una cesión entre organismos de la Administración General del Estado, **se debería haber recabado el consentimiento de los afectados** al ceder los datos a la empresa CISE.

Por lo tanto, el Hospital de Gerona ha cometido una infracción por no recoger el consentimiento para la cesión. Este tipo de infracciones son consideradas de carácter grave o muy grave [Art. 44.3.k y 44.4.b de la nueva modificación de la LOPD].

> [Art. 44.3.k LOPD] Son infracciones graves:
>
> La comunicación o cesión de los datos de carácter personal sin contar con legitimación para ello en los términos previstos en esta Ley y sus disposiciones reglamentarias de desarrollo, salvo que la misma sea constitutiva de infracción muy grave.

> [Art. 44.4.b LOPD] Son infracciones muy graves:
>
> Tratar o ceder los datos de carácter personal a los que se refieren los apartados 2, 3 y 5 del artículo 7 de esta Ley salvo en los supuestos en que la misma lo autoriza o violentar la prohibición contenida en el apartado 4 del artículo 7.

Al tratarse de datos altamente protegidos, relativos a la salud de las personas, se podría considerar la **infracción como muy grave**, lo que supone una sanción de entre 300.001€ y 600.000€ [Art. 45.3 de la nueva modificación de la LOPD].

> [Art. 45.3 LOPD] Las infracciones muy graves serán sancionadas con multa de 300.001 a 600.000 euros.

Como atenuante podría tenerse en cuenta el compromiso de confidencialidad adoptado entre el Hospital y la empresa y rebajar la sanción. Además hay que considerar otros atenuantes (o agravantes) dependiendo de varios factores según se exponen en el artículo 45.4 de la nueva modificación de la LOPD, como pueden ser la intencionalidad o si se han obtenido beneficios por ello. Por lo que la sanción podría bajar a grave únicamente.

> [Art. 45.4 LOPD] La cuantía de las sanciones se graduará atendiendo a los siguientes criterios:
>
> a) El carácter continuado de la infracción.
>
> b) El volumen de los tratamientos efectuados.
>
> c) La vinculación de la actividad del infractor con la realización de tratamientos de datos de carácter personal.
>
> d) El volumen de negocio o actividad del infractor.
>
> **e) Los beneficios obtenidos como consecuencia de la comisión de la infracción.**
>
> **f) El grado de intencionalidad.**
>
> g) La reincidencia por comisión de infracciones de la misma naturaleza.
>
> h) La naturaleza de los perjuicios causados a las personas interesadas o a terceras personas.
>
> i) La acreditación de que con anterioridad a los hechos constitutivos de infracción la entidad imputada tenía implantados procedimientos adecuados de actuación en la recogida y tratamiento de los datos de carácter personal, siendo la infracción consecuencia de una anomalía en el funcionamiento de dichos procedimientos no debida a una falta de diligencia exigible al infractor.
>
> j) Cualquier otra circunstancia que sea relevante para determinar el grado de antijuridicidad y de culpabilidad presentes en la concreta actuación infractora.

De todas formas, si el objetivo del estudio era únicamente una estadística lingüística, deberían haberse enviado los historiales médicos disociados, sin ningún dato que pudiera identificar al paciente (nombre, apellidos, fecha de nacimiento, DNI…). Para recabar datos sobre qué idioma se está utilizando en un historial no hacen falta esos datos personales. Y de esa manera no se tratarían ya de datos protegidos, al estar disociados, ni habría que pedir consentimiento a los afectados [Art. 11.6 LOPD].

> [Art. 11.6 LOPD] Si la comunicación se efectúa previo procedimiento de disociación, no será aplicable lo establecido en los apartados anteriores.

Supuesto II

Introducción

En este segundo supuesto, estamos ante un caso de filtración de datos privados de pacientes del Hospital en una red de distribución de archivos por medio de un software p2p, y es posible que previamente se haya dado un robo de estos datos personales. Habrá que analizar diversos aspectos para establecer si se ha procedido de forma lícita o por el contrario existen irregularidades en algunos procedimientos, bien sea por parte del personal del hospital o de agentes externos.

La primera acción a llevar a cabo es estudiar cómo se ha producido la filtración de datos a eMule. Hay que investigar de dónde han salido esos datos ya que pueden haber sido robados intencionadamente, que se estén almacenando en lugares no seguros o que haya sido un error humano el dejarlos en el ordenador personal de ese empleado.

También hay que investigar quién los ha compartido. Todo parece apuntar al empleado del hospital, pero se necesitará indagar su ordenador para comprobar que realmente ha sido la fuente origen de la filtración. Hay que evaluar la intencionalidad de esta filtración, si existen motivos económicos, rencillas o venganzas personales contra el hospital, etc.

En cualquier caso, hay que evaluar si el hecho de que el empleado desconociese que se estaba compartiendo el archivo a través del emule, le eximiría de responsabilidad o no ante la filtración de datos, y posteriormente si esto serviría como atenuante o agravante de una posible sanción.

Y además de evaluar el cómo, quién y por qué de la filtración, hay que estudiar los hechos "ambientales". Suponiendo que el empleado del hospital ha sido el que ha compartido la información, ¿cómo es que tenía acceso a ella? ¿Qué hacía ese archivo en su ordenador? ¿Su ordenador estaba en un entorno seguro? ¿Estaba autorizado a tener dicha información? Y en caso de estarlo, ¿quién le autorizó? ¿Alguien más tenía acceso a su ordenador?

Por lo tanto, habrá que evaluar la actuación tanto del hospital por la seguridad y procedimientos de almacenado de la información, como del empleado por ser presuntamente el origen de la filtración. A pesar de que la información es escasa se pueden deducir algunos comportamientos indebidos y falta de control de la información.

Estudio del caso

Como venimos viendo en el proyecto, estamos tratando con **datos especialmente protegidos** [Art. 7.3 LOPD]. Al tratarse de datos de las mismas características del supuesto anterior, aplican las mismas medidas de seguridad, tratamiento y cesión expuestas en el supuesto I.

Medidas de seguridad aplicadas por el Hospital

Primero vamos a analizar las medidas de seguridad del Hospital.

En el supuesto I de este proyecto ya se detallaron las medidas de seguridad que se han de cumplir para este tipo de datos, por lo que no se va a duplicar de nuevo aquí dicha lista. Nos centraremos en las medidas que se han incumplido en este supuesto.

El Hospital es probable que cuente (ya que es muy común) con un sistema de usuarios y perfiles, tal y como indican las medidas de seguridad:

> Relación actualizada de usuarios y accesos autorizados.
>
> Control de accesos permitidos a cada usuario según las funciones asignadas.
>
> Mecanismos que eviten el acceso a datos o recursos con derechos distintos de los autorizados.

Por lo tanto, habrá determinados perfiles los que tengan permisos para acceder y copiar los ficheros de datos, pudiendo acotar el origen de la filtración. Sólo un perfil que tuviese acceso a esos datos pudo ser el origen (voluntario o no). Aunque es posible que alguien robase la cuenta a ese usuario.

Entre estas medidas de seguridad citadas, la Agencia de Protección de Datos también indica las siguientes respecto al acceso a los datos:

> Registro de accesos: usuario, hora, fichero, tipo de acceso, autorizado o denegado.
>
> Control de acceso físico a los locales donde se encuentren ubicados los sistemas de información.
>
> Registro de entrada y salida de soportes: documento o soporte, fecha, emisor/destinatario, número, tipo de información, forma de envío, responsable autorizado para recepción/entrega.

Es decir, que el Hospital debería tener registros de acceso a los datos, a los soportes físicos, etc. con los cuales se podría trazar el origen de la filtración, y cómo llegaron esos datos al ordenador del empleado. Por el enunciado del supuesto, aunque no queda totalmente claro, se deduce que pueden no existir tales registros ya que se indica que no se sabe cuál ha sido el origen de la filtración.

En estos registros se almacenaría el usuario, fecha y hora de acceso y tipo de acceso, por lo que se sabría claramente desde qué cuenta de usuario se ha accedido al fichero filtrado, en qué fechas y qué operación se ha hecho (si es un acceso sólo de lectura, una copia, etc..). Con esta información se puede identificar alguna actividad sospechosa, como accesos en horarios no laborales, operaciones no habituales (como copiar el fichero cuando lo normal es simplemente acceder a leerlo). Con esta información es muy probable que se localizara el origen de la filtración, más aún si se ha compartido por eMule desde un equipo del Hospital.

Además, en datos que requieren protección alta como los de este caso, la información debe estar cifrada, por lo que hay otra "negligencia" ya que los datos filtrados estaban en claro (o así se da a entender en el enunciado). Las medidas de seguridad que hacen referencia a este hecho son:

> En ficheros automatizados:
>
> > Cifrado de datos en la distribución de soportes.
> >
> > Cifrado de información en dispositivos portátiles fuera de las instalaciones (evitar el uso de dispositivos que no permitan cifrado, o adoptar medidas alternativas).
> >
> > Transmisión de datos a través de redes electrónicas cifradas.

En el supuesto de que un usuario autorizado hubiera copiado el fichero, y lo hubiera dejado en un equipo al que él mismo o un tercero accedió y compartió el fichero por eMule "sin querer", el daño habría sido mínimo si se hubiera cumplido esta medida que obliga a que se encuentren cifrados los datos. El fichero se habría compartido cifrado, y como mínimo habría pasado un tiempo hasta que alguien lo hubiera descrifrado por fuerza bruta, dando tiempo a la policía a actuar. Al hacerse públicos los datos de forma "inmediata" se entiende que no existía tal cifrado.

Por último, también debe existir un registro de incidencias, según indican las medidas de seguridad:

> Registro de incidencias: tipo, momento de su detección, persona que la notifica, efectos y medidas correctoras.
>
> Procedimiento de notificación y gestión de las incidencias.

Por ello, si se hubiera accedido de forma "forzosa" (un acceso no autorizado) al fichero, para posteriormente publicarlo, debería haberse enviado una notificación al responsable de seguridad indicando los datos de la incidencia, y posiblemente se hubiera atajado el problema antes de que se produjese. Este es otro punto que incumple, presuntamente, el Hospital.

Valoración de la actuación del Hospital

Antes de entrar a valorar si la culpa ha sido del Hospital o de su empleado, se pueden apreciar indicios de **infracción de dos artículos** de la LOPD:

1. [Art. 9.1 LOPD] El responsable del fichero, y, en su caso, el encargado del tratamiento deberán adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados

> y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural.
>
> 2. [Art. 10 LOPD] El responsable del fichero y quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal están obligados al secreto profesional respecto de los mismos y al deber de guardarlos, obligaciones que subsistirán aun después de finalizar sus relaciones con el titular del fichero o, en su caso, con el responsable del mismo.

En el caso del Art. 9.1, se deduce que hay una infracción ya que claramente no se han adoptado las medidas necesarias para garantizar la seguridad de los datos (como hemos analizado en el punto anterior), ya que se han extraviado, filtrado, tratado sin autorización, etc. Además los datos no estaban encriptados para minimizar las consecuencias de un robo.

Del Art. 10 también se deduce que el responsable del fichero (el Hospital en este caso) es el responsable de guardar los datos, al igual que todo aquél que intervenga en el tratamiento de los mismos, como es el empleado del Hospital.

Con la información del supuesto, y siguiendo la hipótesis del "descuido" del empleado del Hospital, parece que no existe intencionalidad ni intereses económicos en la filtración de datos. La filtración parece que se ha debido a un descuido o desconocimiento técnico del empleado, siempre teniendo en cuenta que es una hipótesis y respetando su presunción de inocencia.

Aún así, el hecho de desconocer las tecnologías no eximiría al empleado de la responsabilidad de haber expuesto los datos al público, del mismo modo que el hecho de que haya sido el empleado el responsable de la filtración no exime de su responsabilidad al Hospital, ya que es el responsable de la custodia de los datos.

Por último, se debería investigar para tener en cuenta en este caso el por qué este empleado estaba en posesión de ese fichero en su ordenador (según la información ofrecida en el supuesto entiendo que era un ordenador personal). Habría que investigar si tenía autorización para tenerlo, cómo lo obtuvo, las medidas de seguridad de su ordenador, etc. Lo cual posiblemente derivase en más infracciones, pero formaría parte de una investigación que queda fuera del alcance del proyecto al no disponer de suficiente información.

Conclusiones

El Hospital, como responsable de la custodia y seguridad del fichero de datos, es responsable también de la filtración de los datos.

1. La infracción al artículo 9.1 de la LOPD se establece como grave [Art. 44.3h LOPD]. Esta infracción acarrea una sanción de entre 40.001€ y 300.000€ [Art. 45.2 de la modificación de la LOPD]

    > 1. [Art. 9.1 LOPD] El responsable del fichero, y, en su caso, el encargado del tratamiento deberán adoptar las medidas de índole

> técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural.
>
> 2. [Art. 44.3h LOPD] Son infracciones graves: Mantener los ficheros, locales, programas o equipos que contengan datos de carácter personal sin las debidas condiciones de seguridad que por vía reglamentaria se determinen.
>
> 3. [Art. 45.2 LOPD] Las infracciones graves serán sancionadas con multa de 40.001 a 300.000 euros.

2. La infracción al artículo 10 de la LOPD se establece como muy grave [Art. 44.4b LOPD]. Esta infracción acarrea una sanción de entre 300.001€ y 600.000€ [Art. 45.3 de la modificación de la LOPD].

> 1. [Art. 10 LOPD] El responsable del fichero y quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal están obligados al secreto profesional respecto de los mismos y al deber de guardarlos, obligaciones que subsistirán aun después de finalizar sus relaciones con el titular del fichero o, en su caso, con el responsable del mismo.
>
> 2. [Art. 44.4b LOPD] Son infracciones muy graves: Tratar o ceder los datos de carácter personal a los que se refieren los apartados 2, 3 y 5 del artículo 7 de esta Ley salvo en los supuestos en que la misma lo autoriza o violentar la prohibición contenida en el apartado 4 del artículo 7.
>
> 3. [Art. 45.3 LOPD] Las infracciones muy graves serán sancionadas con multa de 300.001 a 600.000 euros.

Cuando se confirmase la hipótesis de que fue ese empleado el origen de la filtración, se le aplicarían las sanciones oportunas al igual que al Hospital.

En ambos casos se pueden aplicar ciertos atenuantes a las sanciones, como la falta de intencionalidad o que no hubo un motivo económico, al igual que ocurría en el Supuesto I.

Supuesto III

Introducción

En este caso estamos ante lo que puede ser un despido disciplinario legal, o una invasión de la privacidad del empleado. Todo dependerá de que las actuaciones de ambos implicados (Óscar el empleado, y la empresa) hayan sido correctas o no.

Habrá que analizar los hechos y estudiarlos teniendo en cuenta tanto la LOPD como el estatuto de los trabajadores y el código penal si aplicase.

Por una parte habrá que estudiar si es obligatorio para la empresa el tener una política de uso de equipos corporativos en que se indique claramente que éstos sólo podrán usarse para el trabajo y no para el ocio o temas personales.

También habrá que revisar si la empresa ha de comunicar a los empleados que va a instalar una serie de medidas de control para sus equipos.

Después habrá que analizar si la medida adoptada por la empresa es desmedida y agrede la intimidad del empleado. Para ello primero hay que determinar si los datos que recoge la empresa (páginas visitadas, urls, fecha y hora de acceso) son datos de carácter privado o no.

También hay que analizar la actitud del empleado, y ver si puede suponer un despido disciplinario.

Estudio del caso

Para este caso, primero hay que analizar el estatuto de los trabajadores, para entender los derechos de empresario y empleado.

El artículo 5 del estatuto de los trabajadores indica, concretamente son interesantes los apartados a) de cumplir con las obligaciones laborales y la buena fe, c) cumplir las instrucciones del empresario y e) mejora de la productividad.

> [Artículo 5] Deberes laborales.
>
> Los trabajadores tienen como deberes básicos:
>
> a) **Cumplir con las obligaciones concretas de su puesto de trabajo, de conformidad a las reglas de la buena fe y diligencia.**
>
> b) Observar las medidas de seguridad e higiene que se adopten.
>
> c) **Cumplir las órdenes e instrucciones del empresario en el ejercicio regular de sus facultades directivas.**
>
> d) No concurrir con la actividad de la empresa, en los términos fijados en esta Ley.

> **e) Contribuir a la mejora de la productividad.**
>
> f) Cuantos se deriven, en su caso, de los respectivos contratos de trabajo.

Por lo tanto, conductas como por ejemplo ponerse a leer el correo personal, el periódico, juegos, ver películas, etc. son conductas que incumplen los deberes básicos de todo trabajador para con la empresa.

Veamos ahora qué se entiende por **despido disciplinario** y cómo los puntos anteriores pueden conllevar a ello. Tal y como se articula en el artículo 54.2, apartados d y e (trasgresión de la buena fe y abuso de la confianza en el desempeño del trabajo; disminución continuada y voluntaria en el rendimiento del trabajo).

> [Artículo 54] Despido disciplinario.
>
> 1. El contrato de trabajo podrá extinguirse por decisión del empresario, mediante despido basado en un incumplimiento grave y culpable del trabajador.
>
> 2. Se considerarán incumplimientos contractuales:
>
> a. Las faltas repetidas e injustificadas de asistencia o puntualidad al trabajo.
>
> b. La indisciplina o desobediencia en el trabajo.
>
> c. Las ofensas verbales o físicas al empresario o a las personas que trabajan en la empresa o a los familiares que convivan con ellos.
>
> **d. La transgresión de la buena fe contractual, así como el abuso de confianza en el desempeño del trabajo.**
>
> **e. La disminución continuada y voluntaria en el rendimiento de trabajo normal o pactado.**
>
> f. La embriaguez habitual o toxicomanía si repercuten negativamente en el trabajo.
>
> g. El acoso por razón de origen racial o étnico, religión o convicciones, discapacidad, edad u orientación sexual y el acoso sexual o por razón de sexo al empresario o a las personas que trabajan en la empresa.

Vemos que entre los numerosos puntos que pueden provocar un despido disciplinario se encuentran algunos que hacen referencia a precisamente el "perder tiempo en el trabajo", lo cual podría llegar a justificar un despido.

En cuanto a los derechos del empresario, según el artículo 20.3 del estatuto de trabajadores, puede adoptar **medidas de control** del trabajo de sus empleados siempre que se guarde la consideración de la dignidad humana del trabajador.

> [Artículo 20] Dirección y control de la actividad laboral.
>
> 1. El trabajador estará obligado a realizar el trabajo convenido bajo la dirección del empresario o persona en quien éste delegue.
>
> 2. En el cumplimiento de la obligación de trabajar asumida en el contrato, el trabajador debe al empresario la diligencia y la colaboración en el trabajo que marquen las disposiciones legales, los convenios colectivos y las órdenes o instrucciones adoptadas por aquél en el ejercicio regular de sus facultades de dirección y, en su defecto, por los usos y costumbres. En cualquier caso, el trabajador y el empresario se someterán en sus prestaciones recíprocas a las exigencias de la buena fe.
>
> 3. El empresario podrá **adoptar las medidas** que estime más oportunas de vigilancia y control para verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales, guardando en su adopción y aplicación la consideración debida a su dignidad humana y teniendo en cuenta la capacidad real de los trabajadores disminuidos, en su caso.

Con ello se puede entender que el empresario podrá adoptar medidas para asegurar y controlar el trabajo de sus empleados, siempre respetando su dignidad, privacidad (aquí entra la LOPD), etc. Esto se ve confirmado también por el derecho del trabajador según el artículo 4 de Derechos laborales:

> [Artículo 4] Derechos laborales
>
> En la relación de trabajo, los trabajadores tienen derecho:
>
> e) Al respeto de su intimidad y a la consideración debida a su dignidad, comprendida la protección frente al acoso por razón de origen racial o étnico, religión o convicciones, discapacidad, edad u orientación sexual, y frente al acoso sexual y al acoso por razón de sexo.

Ahora vamos a estudiar las actuaciones de cada implicado, antes de valorar en su conjunto si son correctas o no (cosa que haremos en el apartado Conclusiones).

Estudio desde el punto de vista de la empresa

Según el estatuto de los trabajadores como hemos visto, la empresa estaría legalmente autorizada a implantar medidas de control para asegurar que se desarrolla el trabajo correctamente, siempre respetando la dignidad de los trabajadores. Según la LOPD además hay que respetar la intimidad de los mismos, por lo que no se podría leer su correo, ni crear un perfil del mismo por las páginas visitadas por ejemplo. Por lo tanto, de estos dos hechos se deduce que aunque la empresa estuviera en su derecho de establecer medidas de control, lo ha hecho de forma desmedida, sin respetar al empleado.

Analizando con más profundidad la actuación de la empresa, en cuanto a la inspección de las páginas visitadas por el empleado, según el artículo 18 del estatuto de los trabajadores:

> [Artículo 18] Inviolabilidad de la persona del trabajador.
>
> Sólo podrán realizarse registros sobre la persona del trabajador, en sus taquillas y efectos particulares, cuando sean necesarios para la protección del patrimonio empresarial y del de los demás trabajadores de la empresa, dentro del centro de trabajo y en horas de trabajo.
>
> En su realización se respetará al máximo la dignidad e intimidad del trabajador y se contará con la asistencia de un representante legal de los trabajadores o, en su ausencia del centro de trabajo, de otro trabajador de la empresa, siempre que ello fuera posible.

Se establecen unos parámetros a la hora de realizar registros de pertenencias físicas, pero puede extrapolarse al mundo digital, por lo que para realizar la inspección se debería contar con la presencia del representante legal de los trabajadores u otro empleado de la empresa al menos. Dicho esto, podría justificarse que la inspección fuese necesaria (siempre ateniéndonos al estatuto y sin tener en cuenta aquí la LOPD) para proteger el patrimonio de la empresa ya que el hecho de que un trabajador no realiza su trabajo supone pérdidas para una empresa, aunque sería muy estricto.

Si existen realmente razones legales para justificar que el empleado estaba infringiendo su deber con la empresa, se puede proceder a un **despido disciplinario** según articula el estatuto de los trabajadores en el artículo 45:

> [Artículo 45] Causas y efectos de la suspensión.
>
> 1. El contrato de trabajo podrá suspenderse por las siguientes causas:
>
> h) Suspensión de sueldo y empleo, por razones disciplinarias.

Por lo que en dicho caso la actuación de la empresa estaría totalmente justificada y sería legal, si se hubieran obtenido las pruebas de forma legal claro. En ese caso la empresa debería avisar al empleado por escrito, según dicta el artículo 55:

> [Artículo 55] Forma y efectos del despido disciplinario.
>
> 1. El despido deberá ser notificado por escrito al trabajador, haciendo figurar los hechos que lo motivan y la fecha en que tendrá efectos.

En este caso la empresa habría actuado correctamente ya que se avisó al empleado por escrito, adjuntando las pruebas de la decisión de rescindir su contrato.

De todas formas, esto queda invalidado desde el momento en que la empresa obtiene las pruebas de la conducta del empleado de forma ilegítima.

Estudio desde el punto de vista de Óscar

Analizando detalladamente la conducta del empleado, se ve que puede haber vulnerado el artículo 5 del estatuto de los trabajadores expuesto previamente, concretamente los apartados a) de cumplir con las obligaciones laborales y la buena fe, c) cumplir las instrucciones del empresario y e) mejora de la productividad.

Esta actuación podría desencadenar un **despido disciplinario** tal y como hemos visto que se articula en el artículo 54.2, apartados d y e (trasgresión de la buena fe y abuso de la confianza en el desempeño del trabajo; disminución continuada y voluntaria en el rendimiento del trabajo).

Por otra parte, la empresa en ningún momento ha informado al empleado de que se implantaban medidas de control y de qué tipo eran, para verificar que se estaba realizando el trabajo de forma correcta. Y a pesar de ello la empresa ha recogido una serie de información de Óscar para investigarla sin su conocimiento ni consentimiento.

Hay que analizar si estos datos recogidos para controlar a Óscar son datos protegidos por la LOPD para verificar si hay violación de su derecho de intimidad por parte de la empresa. En concreto los datos recogidos son:

- Páginas visitadas categorizadas
- URL
- Fecha y hora de acceso

Para que un dato sea considerado personal ha de cumplir:

1. Que sea información concerniente a una persona física e identificable.
2. Que sea información numérica, alfabética, gráfica, acústica, etc.
3. Que sea información susceptible de recogida, registro, tratamiento o transmisión.

El punto 2 y el punto 3 están claros, pero no así el punto 1. Los datos que indica el supuesto (página, URL, fecha y hora) no son concernientes a una persona identificable. Al menos no por si solos.

Ahora bien, si la empresa le ha presentado al empleado un informe con toda esta información sobre el uso **que ha hecho él** del ordenador corporativo y conexión a Internet, es porque tienen algún otro dato que coteja esta información con el usuario. Por ejemplo, una **IP** que asocia la información a Óscar, un **identificador** de inicio de sesión corporativa, etc. Un dato de ese estilo, que aunque no se ha proporcionado en el informe entregado al empleado, ha de existir sí o sí para poder asegurar que ha sido Óscar quien ha realizado todas esas visitas a esas URL en esas fechas y horas.

De no existir este dato identificador, ¿cómo es capaz la empresa de diferenciar las visitas a páginas de ocio que hace tal o cual empleado? ¿En qué se basa para decir que esas visitas las ha hecho Óscar?

Por lo tanto, al existir un dato que asocia las visitas a una persona física, identificable, esta información pasa a ser **personal**, y a estar bajo la protección de la LOPD.

Conclusiones

Considero que, aunque la actitud del empleado pudiera justificar un despido disciplinario, la forma de actuar de la empresa no ha sido correcta.

Según la LOPD, la empresa ha recogido datos personales de un empleado sin su consentimiento y sin informarle debidamente de que la empresa adoptaría esas medidas de control, sin tratar dichos datos como datos personales, estará incurriendo en un **delito contra la intimidad** de la persona, tipificado en el código penal artículo 197.1 *"intercepción de las telecomunicaciones"*.

> [Artículo 197] Código penal
>
> 1. El que, para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere de sus papeles, cartas, mensajes de correo electrónico o cualesquiera otros documentos o efectos personales o intercepte sus telecomunicaciones o utilice artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación, será castigado con las penas de prisión de uno a cuatro años y multa de doce a veinticuatro meses.

Primero debería de informar a sus empleados de las medidas de control que va a llevar a cabo para controlar el uso de los PCs. De querer almacenar y tratar datos personales de navegación debe informar de su uso a los afectados, registrarlos en un fichero en la Agencia de Protección de Datos, y adoptar las medidas de seguridad adecuadas para su custodia.

Al haber **agredido la intimidad** de Óscar, la empresa ha cometido un delito (artículo 197.1 del código penal como expuse antes). Se cumplen las condiciones para considerar estos actos ilícitos:

1. Que se hagan sin el consentimiento del afectado.
2. Que se lleven a cabo con la intención de descubrir los secretos o vulnerar la intimidad ajena.

Se han hecho sin consentimiento del afectado puesto que ni siquiera se ha informado de las medidas de control de la empresa. Y obviamente tienen como intención descubrir "los secretos" de la intimidad del empleado, para descubrir qué páginas visitaba.

Además, hay que tener en cuenta que aunque esos datos parezcan decir poco de una persona, realmente se puede obtener un perfil muy completo de un individuo conociendo 5556 páginas que ha visitado. Existiendo webs de salud, juegos, financieras, medicina, redes sociales... se puede extraer información como orientación sexual, situación financiera, estado de salud...

No es seguro que se pueda extraer ese tipo de información pero sí probable. Por lo tanto los datos podrían ser incluso considerados de protección especial. Aunque esto requeriría un estudio profundo de la información y conocimientos y experiencia en temas legales más extensos.

Existen **otros mecanismos** tanto para prevenir la actuación de Óscar como para detectarla, sin afectar ni invadir su privacidad. Por ejemplo, existen numerosas soluciones software que impiden el acceso a determinadas webs, pudiendo bloquear en un puesto de trabajo las webs relacionadas con el ocio, y así evitando la conducta de Óscar. También hay otros mecanismos que podrían detectar que un empleado está haciendo un uso no adecuado de su ordenador, pero sin indicar ni almacenar exactamente qué webs visita etc. En este caso se debería previamente informar al trabajador de que existe esta medida, para su conocimiento y que actúe en consecuencia.

Por lo tanto, se ha realizado un **despido improcedente** a Óscar, y por tanto el empresario deberá, según el estatuto de los trabajadores (y a parte de las sanciones por parte de la LOPD):

> [Artículo 56] Despido improcedente.
>
> 1. Cuando el despido sea declarado improcedente, el empresario, en el plazo de cinco días desde la notificación de la sentencia, podrá optar entre la readmisión del trabajador, con abono de los salarios de tramitación previstos en el párrafo b) de este apartado 1, o el abono de las siguientes percepciones económicas que deberán ser fijadas en aquélla:
>
> ---
>
> a. Una indemnización de cuarenta y cinco días de salario, por año de servicio, prorrateándose por meses los períodos de tiempo

> inferiores a un año hasta un máximo de cuarenta y dos mensualidades.
>
> b. Una cantidad igual a la suma de los salarios dejados de percibir desde la fecha de despido hasta la notificación de la sentencia que declarase la improcedencia o hasta que hubiera encontrado otro empleo, si tal colocación fuera anterior a dicha sentencia y se probase por el empresario lo percibido, para su descuento de los salarios de tramitación.
>
> 2. En el supuesto de que la opción entre readmisión o indemnización correspondiera al empresario, el contrato de trabajo se entenderá extinguido en la fecha del despido, cuando el empresario reconociera la improcedencia del mismo y ofreciese la indemnización prevista en el párrafo a) del apartado anterior, depositándola en el Juzgado de lo Social a disposición del trabajador y poniéndolo en conocimiento de éste.
>
> Cuando el trabajador acepte la indemnización o cuando no la acepte y el despido sea declarado improcedente, la cantidad a que se refiere el párrafo b) del apartado anterior quedará limitada a los salarios devengados desde la fecha del despido hasta la del depósito, salvo cuando el depósito se realice en las cuarenta y ocho horas siguientes al despido, en cuyo caso no se devengará cantidad alguna.
>
> A estos efectos, el reconocimiento de la improcedencia podrá ser realizado por el empresario desde la fecha del despido hasta la de la conciliación.
>
> 3. En el supuesto de no optar el empresario por la readmisión o la indemnización, se entiende que procede la primera.
>
> 4. Si el despedido fuera un representante legal de los trabajadores o un delegado sindical, la opción corresponderá siempre a éste. De no efectuar la opción, se entenderá que lo hace por la readmisión. Cuando la opción, expresa o presunta, sea en favor de la readmisión, ésta será obligada.

Por lo que el empresario deberá o readmitir al empleado o indemnizarle.