



TRABAJO DE INVESTIGACIÓN

CARMEN XIA MARTINEZ ESPINOSA
1º GESTIÓN DE LA CIBERSEGURIDAD

Breve descripción

En el siguiente trabajo hablaremos de la problemática de las cookies ante la ignorancia o desconocimiento de los usuarios.

ÍNDICE

Contenido

Introducción y contexto	3
1. La aceptación de las cookies en aplicaciones de nuestro día a día.	4
Controversia por los Riesgos de las cookies.....	5
2. Ley de cookies y su aplicación en España.	6
Conceptos previos.....	6
La ley de cookies de la UE y su contenido actual	6
Su aplicación en España.	6
¿Quién es el responsable de la gestión de las cookies en una página web?	7
¿Cuál es la legitimación para el uso de las cookies?	7
3. La violación de nuestro derecho de intimidad como derecho fundamental....	8
La intimidad digital.....	8
Desconexión digital	9
4. La ley de protección de datos y su infracción.	10
¿Qué es la ley de protección de datos?	10
¿Cómo lo podemos aplicar a las cookies?.....	10
Su infracción.....	11
Bibliografía.....	12

Introducción y contexto

Antes de todo, no debemos dejar a un lado para introducirnos en este tema, nuestro punto central, las cookies. ¿Qué son las cookies?

Bien, se puede decir que las llamadas ``cookies`` son usadas para poder navegar de una mejor forma por la red, descrito así por el Consejo de la Unión Europea.

De otra manera, las podemos definir como el modo que implantan los sitios web en nuestro dispositivo móvil u ordenador para poder reconocer nuestro modo de navegar y preferencias para poder facilitar así a la hora de volver a visitar la página que esta no la tenga que volver a configurar.

En conclusión, las cookies son usadas por los sitios web para ofrecer de manera personalizada información a los usuarios.

En cuanto a la regulación de estas en nuestro país, se encuentra en el artículo 22.2 de la Ley 34/2002 del 11 de julio, de Servicios de la Sociedad de la información y de Comercio electrónico.

Por ello, sabiendo sus intenciones, debemos pasar a hablar sobre la problemática y la ignorancia de algunos en cuanto a su aceptación, la ley de cookies, la ley de protección de datos y la posible violación de nuestro derecho de intimidad como derecho fundamental.

1. La aceptación de las cookies en aplicaciones de nuestro día a día.

Para ponernos en contexto en cuanto al dictamen del Reglamento General de Protección de Datos, declara las intenciones del legislador europeo, en cuanto a la protección de datos. Sin embargo, con nuestro tema a desarrollar, las cookies, no sucede así.

Como hemos dicho anteriormente, las cookies son impuestas por el propietario de la página web por la que navegamos o incluso por terceros. Por lo que nuestra privacidad quedaría expuesta. Pero..., nos encontramos ante esta pregunta, ¿para que el consentimiento sea válido, como se debe de consentir el control y manejo de nuestra propia información?

Para poder entenderlo mejor y aplicarlo a una situación de la vida real, podemos poner de ejemplo cuando entramos en Instagram, Facebook, tiktok o alguna red social o página web ¿Por qué debo aceptarlas? ¿Si o no?

Tomaremos como ejemplo nuestro inicio de sesión en Instagram, una de las redes más famosas y usadas entre los jóvenes, hoy en día. Puede que no recuerdes, pero al registrarte por primera vez en Instagram, te apareció un texto en mitad de la pantalla donde pulsaste ``acepto``.

Para poder enumerar todas las cookies que expone Instagram, deberíamos al menos leernos trescientas páginas, pocas personas o ninguna se paran a leerlas. Por ello también debemos conocer los riesgos que ello supone.

Aplicándolo a nuestro ejemplo, Instagram usa las cookies para que se guarde en tu dispositivo móvil, ordenador o navegador información personal y preferencias (si usas o no el modo oscuro, el idioma que hablas y el país donde vives, el contenido que buscas habitualmente...)

Ahora, nos cuestionamos si debemos o no aceptarlas, ¿debemos?

Podemos encontrar algunas ventajas o desventajas para responder a esta pregunta; Instagram con su aceptación puede mostrarte personalmente para ti contenido y anuncios publicitarios que en el momento en el que estés usando la aplicación te interesen.

Los que están en contra de las cookies culpan a la red social de usar estos archivos para obtener beneficios mediante esta información personal, algo cierto, ya que al aceptarlas siendo ignorantes del ``contrato`` que estamos aceptando, nuestras preferencias y contenido se comparten con anunciantes y ajenos para mejorar la visualización de contenido de la red social.

Controversia por los Riesgos de las cookies.

Hablemos de riesgos y privacidad, aunque la privacidad la trataremos más en profundidad en páginas siguientes.

Se ha dicho innumerables veces los riesgos que conlleva el uso del internet y lo peligroso que es, pero el uso depende mucho de clasificar el internet como peligroso y seguro.

Por ello, en este tema relacionado con las cookies, depende mucho como se utilicen las cookies y como se expongan, pueden o no producir riesgos a los usuarios de la red de diferentes maneras. Aquellos navegadores que permiten el uso de cookies pueden permitir su uso para determinar tu ruta en internet y desafortunadamente en determinados casos acabar en manos de quien no queremos que acaben.

Se debe concienciar a las personas del cuidado que se debe de tener al aceptar o permitir las cookies, porque con un solo clic en un enlace desconocido puede provocar fatales consecuencias para tu propia privacidad.

La controversia de este tema sobre la defensa de la privacidad y seguridad de las personas en la red ha generado que se desarrollen algunas leyes especiales para esto para poder controlar y evitar malos usos de ellas y el abuso de la información, de aquí la conocida Ley de Protección de Datos y la Ley de Cookies.

Como conclusión propia acerca de su aceptación o no, en aspectos digitales cotidianos, depende de cada uno y de su consciencia acerca de su propia seguridad y uso. Pero hago hincapié en la necesidad de fomentar el conocimiento de las cookies para un mayor sentimiento de seguridad de los usuarios.

<https://blog.alana.ai/es/alana-por-la-innovacion/cookies-definicion-riesgos-privacidad/>

<https://androidphoria.com/aplicaciones/aviso-de-cookies-instagram>

2. Ley de cookies y su aplicación en España.

Conceptos previos

Debemos visualizar unos conceptos previos antes de aplicarlos a la ley.

La ley de cookies, la que nos sale cuando entramos en una página web o como hemos expuesto antes al iniciar sesión en alguna red social.

Antes de todo, debemos saber el concepto de la ``ley de cookies``, es aquella que informa de una forma clara y detallada cual es el objetivo de la cookie y su fin, que tipo usamos, como desactivarlas y configurarlas.

El Parlamento Europeo, con el propósito de garantizar y fortalecer la protección de los datos privados y personales de los usuarios y que se encontrase dentro del marco legal de los Estados que forman parte de la UE, introdujo esta nueva ley.

El Tribunal de Justicia de la Unión Europea, en una sentencia, dictó el consentimiento para la instalación de las cookies en los dispositivos de los usuarios web. Hace relativamente poco, sobre el año 2018, desde entonces, las empresas como hemos dicho anteriormente se ven obligadas a informar al usuario sobre el uso de esta política de cookies y su aceptación, previamente a proceder con un solo clic a aceptarlas.

La ley de cookies de la UE y su contenido actual

La UE, pretende proteger o dar una mayor protección a los datos privados y personales de los usuarios de la red. Dentro de esta ley, se distinguen dos tipos de cookies.

- Necesarias: son las llamadas ``necesarias`` para el correcto funcionamiento de la web. Ejemplos claros serían el inicio de sesión automático, cuando pulsamos el ``recordar la sesión``. Al finalizar y cerrar por ejemplo el navegador (Google), se cerraría la sesión.
- No necesarias: recopilan otro tipo de información. Ejemplos:
 - o Redes sociales, comportamiento de los usuarios, adaptación de los anuncios al usuario y recopilación como por ejemplo la ubicación.

Su aplicación en España.

La ley de cookies publicada en el Real Decreto en marzo de 2012, se consideró una ley de cumplimiento obligatorio, la cual si incumples debes cumplir una sanción.

En ella se expresaba la necesidad de tener en cuenta la aceptación del usuario a ellas.

Se han ido actualizando mediante la Guía de Usuario de las cookies, donde se recuerda:

- Consentimiento informado de los usuarios previos a la instalación de los ``archivos`` de las cookies.
- La facilidad o facilitar la transparencia de la información a los usuarios. Es decir, informar de una manera clara.

Ya que cada vez somos más conscientes del cambio tecnológico y nuestra dependencia a ellas. Debemos preocuparnos por las Cookies y protección de datos, preguntándonos; ¿Qué será de ellas en el futuro?

Bien, todos los propietarios y administraciones de páginas web, deberán actualizarse en términos legales en cuanto a la ley de cookies. Un nuevo reglamento ePrivacy, tiene mayoritariamente disposiciones que tratan sobre datos privados y personales de los usuarios.

¿Quién es el responsable de la gestión de las cookies en una página web?

Todas las páginas web deben tener el llamado Aviso Legal, es aquel donde se puede acceder al tratamiento de las cookies por el titular o propietario de la web.

De una forma más detallada y técnica, definimos el Aviso Legal como aquel documento legalizado ubicado dentro del sitio o página web que identifica a su propietario. La Ley de Servicios de la información, obliga a que se incluya este aviso en prácticamente todas las webs. También incluye otros datos obligatorios a incluir en estas páginas.

¿Cuál es la legitimación para el uso de las cookies?

Respecto a las cookies en general, como dijimos en líneas anteriores, es el propio usuario el que decide o no aceptarlas, su consentimiento.

En caso de negarse a aceptarlas no producirá ningún problema a la hora de navegar por internet o esa página web o red social concreta. Su función de personalizar la navegación no se llevará a cabo, por lo que el tratamiento de datos realizados anteriormente no se perderá o dejarán de ser lícitos por la simple acción de revocar el consentimiento.

3. La violación de nuestro derecho de intimidad como derecho fundamental.

Conforme a nuestra Constitución en el Título I de los derechos y deberes fundamentales, en el segundo capítulo Derechos y Libertades del Título I De los derechos y deberes fundamentales. El artículo 18 dice lo siguiente.

Se garantiza el derecho a:

1. Honor.
2. Intimidad personal y familiar
3. Propia imagen.

Dice también que el domicilio es inviolable y para su entrada o registro se requiere; resolución judicial o consentimiento del titular.

“También se limitará el uso de la información para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos. (“TEMA 5. LOS DERECHOS AL HONOR, A LA INTIMIDAD Y A LA PROPIA IMAGEN - UCA”)

Por último, garantiza la confidencialidad de las comunicaciones en especial.

Consideramos pues el derecho de intimidad como un derecho fundamental de nuestra Constitución.

A continuación, vamos a hablar de nuestro derecho de intimidad aplicado a la intimidad en internet. Como hemos dicho en páginas y párrafos anteriores, actualmente vivimos en una sociedad digitalizada. Total, o parcialmente compartimos datos e información en internet. Por menor que sea tu uso del internet, has compartido inconsciente o conscientemente información.

Podemos volver a usar los ejemplos usados anteriormente, pensemos cuando nos registramos en cualquier página web, plataformas de video online como Netflix o redes sociales como las más habituales Facebook, Twitter e Instagram.

La intimidad digital.

Hablemos entonces de la intimidad digital, que es definida como la cantidad de información personal e íntima de las personas que, aunque no sea visible, circulan por la red.

Por lo que con determinadas leyes se debe regular cuales son los términos en los que las empresas pueden y no hacer cuando nosotros facilitamos datos personales en sus webs iniciando sesión.

El Derecho a la intimidad está relacionado con la desconexión digital, está regulado además en una Ley Orgánica 3/2018.

Desconexión digital

Es cierto, que tras la pandemia de COVID 19, nuestra forma de relacionarnos ha cambiado drásticamente, ha marcado un antes y un después.

Es preciso aclarar lo que es el derecho a la desconexión digital. Se considera un derecho laboral de los empleados. Como su nombre bien indica ``desconexión digital``, quiere decir; no conectar nada digital que tenga que ver con el trabajo o que lleve inaugurado el software de la empresa. Por ejemplo, si en nuestra empresa tenemos un dispositivo móvil habilitado para recibir llamadas, correos y mensajes relacionadas con la empresa, durante nuestro periodo vacacional o fuera del ámbito laboral y del horario de trabajo, estamos en nuestro total derecho de no contestar.

Pero es cierto que, siendo realistas, este derecho sigue pasando por desapercibido. Según una investigación *``InfoJobs asegura que el 75% de los trabajadores españoles responden llamadas o emails fuera del horario laboral``* Fuente: Metropol Abogados. (Metropolabogados.com derecho a la desconexión digital).

Como afectan las cookies a este derecho.

Las cookies si afectan a nuestra privacidad, por ello se insiste tanto en el cumplimiento de la normativa al instalarse en nuestro ordenador. Pero también debemos cuestionarnos si esas características y requisitos son suficientes para la correcta protección de nuestros datos y privacidad, planteándonoslo aún mas cuando se trata de las cookies de terceros y la repercusión que supone por si esos datos personales llegan a manos de otros.

Porque realmente como ya hemos dicho, la libertad es un derecho fundamental, al igual que las cookies se determinan seguras, dependiendo eso sí del uso que le demos y de nuestro propio criterio para aceptarlas,

4. La ley de protección de datos y su infracción.

¿Qué es la ley de protección de datos?

Es más conocido como el Reglamento General de Protección de Datos. Como su nombre indica, protege los datos personales de los usuarios. Tanto en las empresas como en páginas web deben de tener en cuenta los principios y características de esta ley.

Según esta ley, los legisladores europeos deben proteger los datos personales. Consideramos como ``dato personal`` es toda información que tiene la capacidad de identificar a una persona.

¿A quién afecta esta ley? Se aplica por un lado a todos los Estados Miembros y a las empresas mundiales que traten datos personales de personas europeas. También se aplica a todas las empresas españolas.

En cuanto a su aplicación debemos tener en cuenta dos cosas o figuras:

- el responsable de tratar datos personales: es la persona que toma las decisiones sobre el tratamiento a realizar y su fin relacionado con los datos personales en el ámbito comercial.
- el encargado del tratamiento de datos personales: tiene total acceso a aquellas bases donde se hayan los datos personales.

Por lo tanto, concluimos que la Ley de Protección de datos regula el trato de nuestros datos personales tanto aplicado en el ámbito digital como en nuestra vida cotidiana. Todo ello para evitar riesgos como fraude, acoso, extorsión. Por ello, debemos concienciarnos de un buen uso responsable de la información, en resumen, proteger nuestra información personal y datos mediante todas las posibilidades disponibles.

¿Cómo lo podemos aplicar a las cookies?

Bien, pues el RGPD (Reglamento General de Protección de Datos), es aquella legislación de la Unión Europea que se encarga de regular toda aquella información y datos personales de las personas que se encuentran dentro de la Unión Europea.

Por lo tanto, según este Reglamento, la responsabilidad legal de los sitios web es de los propietarios y sus operadores. Recalcar de nuevo que, aunque un sitio web se encuentre fuera de ella, debe cumplir el reglamento si trata datos personales de una persona europea.

Las cookies según el RGP exigen que solo para obtener determinados fines y con el consentimiento del usuario la web recoja datos personales de sus usuarios.

También distingue cuatro tipos de cookies o cuatro categorías, las necesarias, las de preferencia, estadísticas y de marketing. De hecho, dice también que

aquellas cookies que no sean necesarias totalmente para que la página web funcione deben activarse solo después de que se haya dado el consentimiento de los usuarios solo para ese fin específico.

Una política de cookies según este reglamento debe informar a los usuarios de:

En conclusión y como resumen de este reglamento aplicado a las cookies, es que el consentimiento del usuario debe ser claro y explícito, y libre, es decir no estar condicionado a ningún tipo de servicio.

Su infracción.

“Toda violación de la seguridad que ocasione destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizado a dichos datos”
 (“Vulneración de la protección de datos ¿Qué debemos hacer cuando sucede ...”) (“RGPD Q&A: Violaciones de Seguridad de los Datos Personales”)

¿Cuándo se vulnera entonces la ley de Protección de Datos?

Como hemos dicho en el párrafo anterior, ahí de esa manera se vulnera, o cuando una persona ajena tiene total acceso a datos personales, o cuando hay una negligencia o error en el trato de información, cuando hay un descuido, un ataque por hackers a la web (ciberataque)... En conclusión, cualquier otro motivo que se encuentre en el RGPD (tratado en párrafos anteriores).

Un ejemplo; la sanción de 2.100.000 euros que recibió CaixaBank por enviar comunicaciones comerciales de los usuarios ofreciéndoles a cambio la anulación o eliminación de las comisiones de su contrato bancario. Es decir, condicionaron su consentimiento.

Podemos concluir pues, que las sanciones por la vulneración de la protección de datos, tanto de forma involuntaria, voluntaria, por un ciberataque o muchos motivos más, se establecen unas sanciones desde 40.000 hasta 20 millones de euros en casos muy graves.

En caso de que seamos nosotros los vulnerados, solicitaremos mediante la justicia una indemnización por la violación de la protección de datos, siempre presentando la causa y pruebas que lo verifiquen.

Para que se eviten estas vulneraciones, se debe pedir el asesoramiento especializado de una consultoría de protección de datos. Para que te asesore en cuanto a la aplicación de medidas técnicas adecuadas para evitar estas situaciones.

Bibliografía

[Dialnet-InformaticaYLibertad-26680.pdf](#)

[Uso de cookies \(www.derechoshumanos.net\)](#)

[file:///C:/Users/Xia%20Martinez%20Espinosa/Downloads/Dialnet-LasCookies-4730460.pdf](#)

Ref: <https://adefinitivas.com/arbol-del-derecho/modelo-aviso-legal-a-definitivas/>

<https://letslaw.es/ley-de-proteccion-de-datos/>

<https://digestum.es/cookies-como-afectan-privacidad/>

<https://metropolabogados.com/2022/06/29/que-debes-saber-sobre-derecho-a-la-desconexion-digital/>

<https://blog.alana.ai/es/alana-por-la-innovacion/cookies-definicion-riesgos-privacidad/>

<https://androidphoria.com/aplicaciones/aviso-de-cookies-instagram>

<https://www.ionos.es/digitalguide/paginas-web/derecho-digital/la-ley-de-cookies-y-su-aplicacion-en-espana/>

<https://protecciondatos-lopd.com/empresas/vulneracion/>

<https://digestum.es/cookies-como-afectan-privacidad/>

<https://www.cookiebot.com/es/rgpd-cookies/>