Universidad de Valparaíso

Facultad de Derecho y Ciencias Sociales

Escuela de Derecho

LAS COOKIES Y SU REGULACIÓN EN NUESTRO ORDENAMIENTO JURÍDICO: UNA PERSPECTIVA GENERAL EN RELACIÓN CON EL TRATAMIENTO Y PROTECCIÓN DE DATOS PERSONALES.

Autora:

Camila Rivera Gallardo

Profesor guía:

Patricia Reyes Olmedo

Diciembre 2023

Abstract:

El tratamiento en nuestro ordenamiento jurídico de las cookies, es un aspecto que ha cobrado importancia a propósito de un informe técnico realizado por parte del SERNAC el año 2022, cuya finalidad era identificar los problemas que existen en el consentimiento de los usuarios o consumidores y que demostró como se ve vulnerando el principio de protección de los datos personales consagrado en Artículo 19 n°4 CPR, por parte de distintas entidades (tanto públicas como privadas) y como la Ley 19.628 ha resultado insuficiente para prevenir estás situaciones. El texto, en base al análisis que otros sistemas y organismos internacionales que han desarrollado principios y políticas frente a las cookies, busca analizar cómo el nuevo proyecto de Ley sobre "Protección de Datos personales" permitirá un mejor resguardo al problema del consentimiento. **Palabras claves:** Cookies- SERNAC- 19 n°4 CPR- Ley 19.68- Protección de datos personales- Consentimiento.

Índice

Introducción 4

Capítulo I: Aspectos generales de las cookies 5

1.1 Definición y evolución de las cookies 5

1.2 Clasificación de las cookies 6

1.3 Algunos Conceptos claves 7

1.4 Diferencias entre las cookies y la memoria caché 8

1.5 La utilización de cookies por parte de organismos públicos 8

1.6 La utilización de cookies en redes sociales 10

1.7 La utilización de las cookies por proveedores de tecnología 11

Capítulo II: Directrices generales OECD y principios generales sobre la protección de datos personales. 14

2.1 Directrices generales OCDE 14

2.2 Principio de Consentimiento libre, informado e inequívoco. 15

2.3 Principio de autodeterminación informativa. 16

2.4 Principio de neutralidad en la red o Acceso a la libertad de navegación web 18

2.6 Sanciones aplicadas por órganos internacionales a la utilización de cookies. 19

2.7 Proyecto de ley "protección de datos personales" en relación con las cookies 20

Capítulo III: Regulación de las cookies en nuestro ordenamiento jurídico y resguardo al Artículo 19 n°4 CPR 22

3.1 Ley N°19.628 sobre la protección de la vida privada. 22

3.3 Resguardo derecho fundamental a la protección de datos personales Art 19 N°4 CPR y Limitación o restricción al acceso a la información. 23

Capítulo IV: Las cookies y su relación con la IA, desafíos para el Derecho 25

4.1 Aplicación de Inteligencia Artificial (IA) a las cookies y su ayuda a la ciberseguridad. 26

Conclusiones 28

Bibliografía 30

Introducción

El avance tecnológico ha traído consigo una serie de desafíos a las distintas legislaciones de los países, que buscan día a día adaptar sus normativas a este avance progresivo, siendo el sistema implementado por la Unión Europea el que se encuentra más avanzado en relación con la protección de datos personales, pero igualmente ha resultado ser insuficiente para los peligros que supone la ciberseguridad.

En ese contexto, las cookies han resultado ser un problema que ha ido tomando relevancia, dado el escaso tratamiento que se le daba como un mecanismo de recolección de información y cómo los distintos proveedores de servicios lo utilizan indiscriminadamente para la creación de perfiles de sus usuarios.

La Unión Europea frente a los compromisos adquiridos en distintos acuerdos y tratados ha logrado cumplir con los estándares que se han sugerido por distintos órganos internacionales, teniendo actualmente un Reglamento General sobre Protección de Datos Personales que regula las cookies.

Por nuestra parte, Chile actualmente no ha implementado de manera integral las sugerencias planteadas por los organismos internacionales sobre protección de datos personales, incumpliendo sus compromisos, por ejemplo, no ha incorporado de manera expresa los principios asociados a la protección de datos personales, debiendo realizarse una interpretación extensiva de ellos, además de no contar con un marco regulador que nos indique hasta qué punto es recomendable la entrega de datos personales y cuales serian las limitaciones con las que se contarían para esto.

Por lo anterior, en esta tesina se buscará dar cuenta de la regulación de las cookies, no solo en nuestro ordenamiento jurídico, sino el tratamiento que le dan los organismos internacionales y otros sistemas, (Unión Europea y Estados Unidos) con la finalidad de establecer un panorama actual y como a futuro esto puede cambiar con la aprobación e implementación del proyecto sobre datos personales, actualmente en tramitación.

Capítulo I: Aspectos generales de las cookies

1.1 Definición y evolución de las cookies

Las cookies son fragmentos de textos que se utilizan para conservar información en navegadores web y se usan para almacenar y recibir identificadores y otros datos en computadores, teléfonos y otros dispositivos. Es decir, a través de su uso, los proveedores de un sitio web pueden obtener datos relacionados con sus usuarios (Debusseré, 2005 citado por SERNAC, 2022, p.5).

La creación de las cookies data de la década de los 90, donde se crean con la finalidad de identificar a los usuarios y sus patrones de conducta en la realización de visitas a un sitio web determinado, conociéndose con el nombre de "persistent client state object". Posteriormente, fue adoptado el nombre de cookies, este término deriva de la palabra en inglés "magic cookies" que proviene del área de la informática, siendo actualmente el nombre con que se le conoce. De esta manera, podemos señalar que: *La cookie fue inventada por Lou Montulli, empleado de Netscape Communications en junio de 1994 durante el desarrollo de una solución de eCommerce para MCI Inc. (Empresa de Telecomunicaciones que fue, durante varios años, la segunda operadora de larga distancia más grande en US)* (Torija, 2021). En el año 1995 esta idea es patentada y vendida a internet explorer comenzando de esta manera su masificación.

Las cookies funcionan de la siguiente manera según lo ha señalado el Profesor Iñigo De la Maza: *Cada vez que Ud. abre una página web en su navegador o browser envía a esa página cierta información necesaria para proveerle acceso (...), el servidor responde enviando el HTTP y el código HTML, lo que le permite bajar la página [web] a su computador. Pues bien, inserto en el código HTML de algunas de las páginas que Ud. visitó y que poseían banners de avisaje, existía un enlace invisible a la compañía que administra esos banners y que es capaz de rastrear las cookies de esa compañía que su computador tiene o, en caso de que no tenga, insertárselas* (Michea, 2022, p.511.)

Actualmente, las cookies son una herramienta indispensable utilizada por la gran mayoría de sitios web con la finalidad de prestar un servicio personalizado a sus usuarios, aunque no siempre es el único objetivo que persiguen. Esto queda en evidencia en el estudio realizado por SERNAC en el año 2019, donde analizaron el comportamiento de 187 proveedores pertenecientes al rubro del comercio electrónico. Los estudios arrojaron los siguientes resultados:

Se detectó que el 80% de ellos utilizan cookies que les permiten analizar el comportamiento de los consumidores y elaborar su perfil. Además, el 62% de las empresas que utilizan cookies declaró almacenar la información recogida por sus cookies y entre dicha información se encuentran características personales de los consumidores (90,7%), el

perfil de comportamiento del consumidor (70,1%), su tráfico de navegación (62,9%) e información sobre las publicidades visitadas (44,3%) (Radiografía Del Comercio Electrónico, 2019). Este estudio ratifica el impacto para las empresas como mecanismo de recopilación y almacenamiento de datos, con el objetivo de esclarecer los patrones de comportamiento de sus usuarios, pero también el grado de riesgo o exposición que se encuentran los datos personales sin la debida entrega de información sobre el uso o tratamiento que realmente se les va a dar.

1.2 Clasificación de las cookies

Las cookies son herramientas esenciales para la recopilación y almacenamiento de datos personales, por lo mismo, los diferentes proveedores de servicios le dan diferentes usos según sus necesidades y por esta razón también su finalidad. Los almacenamientos que desarrollarán dependen del tipo de cookies a las cuales nos refiramos, dado que existen distintos tipos. Siguiendo al Consejo para la Transparencia y su política de cookies, podríamos señalar que existen nueve tipos de cookies distintas, las cuales a su vez se pueden clasificar según: A) La entidad que las gestiona B) el plazo de tiempo que permanezcan activadas. C) Según la finalidad que tengan.

A) Según la entidad que la gestiona:

Cookies propias: *son aquellas que se envían a su dispositivo desde nuestros propios equipos o dominios.*

Cookies de terceros: *son aquellas que se envían a su dispositivo desde un equipo o dominio que no es gestionado por nosotros, sino por otra entidad colaboradora.*

B) Según el plazo de tiempo que permanecen activadas:

Cookies de sesión: *son cookies temporales que permanecen en el archivo de cookies de su navegador hasta que abandona la página web, momento en el que son eliminadas.*

Cookies persistentes: *son almacenadas internamente en su dispositivo incluso al finalizar la navegación web, y son objeto de consulta cada vez que realiza una nueva visita. Una cookie permanente posee una fecha de expiración determinada, llegada la cual dejará de funcionar.*

C) *Según su finalidad:*

Cookies técnicas: *son aquellas que permiten la ejecución de funcionalidades, opciones o servicios de la web vinculadas a los propios servicios de la misma como, por ejemplo, controlar el tráfico y la comunicación de datos,*

identificar la sesión, contar visitas, utilizar elementos de seguridad durante la navegación, o compartir contenidos a través de redes sociales.

Cookies de preferencias o personalización: *son aquellas que permiten acceder al servicio con unas características predefinidas en función de criterios determinados por el responsable de la web, como por ejemplo el idioma, el tipo de navegador a través del cual se accede al servicio, su configuración regional, etc.*

Cookies de análisis o medición: *son aquellas que nos permiten cuantificar el número de usuarios, visitas o acciones, y así realizar la medición y análisis estadístico y cuantitativo de la utilización que hacen los usuarios de la web y sus contenidos.*

Cookies publicitarias: *son las que permiten gestionar el funcionamiento de los espacios e inserciones publicitarias, sin tener en cuenta un perfilado específico del usuario.*

Cookies de publicidad comportamental: *son aquellas que almacenan información relacionada con el comportamiento de los usuarios obtenida a través de la observación continuada de sus hábitos de navegación, lo que permite desarrollar un perfil específico para mostrar publicidad en función de este.* (Consejo para la Transparencia, 2021)

Es posible que las cookies utilizadas por los sitios web se encuentren en una sola clasificación, pero en la mayoría de los casos pertenecen a más de una categoría o clasificación. Teóricamente, para el correcto funcionamiento de las páginas se requiere únicamente de la utilización de cookies esenciales o técnicas.

1.3 Algunos Conceptos claves

Los conceptos presentados a continuación, definidos por SERNAC, tienen relación con la configuración por defecto y la paradoja de la privacidad:

Configuración de adhesión voluntaria (opt-in): *Presenta las opciones de configuración de todas las cookies - necesarias y adicionales - teniendo solamente seleccionadas por defecto las cookies necesarias para el funcionamiento del sitio web y del presente estudio. Esto está acompañado de un botón de respuesta que resalta la opción de "aceptar seleccionadas". De esa manera, mediante el diseño por defecto se promueve o facilita la protección de datos personales.* (SERNAC, 2022, p.53)

Configuración de exclusión voluntaria (opt-out)*: Utiliza el mismo botón que el caso anterior, pero todas las cookies adicionales están seleccionadas por defecto. En caso de que el usuario no quiera suscribir las cookies*

adicionales, tendrían que activamente desmarcar las opciones por defecto. De esa manera, mediante el diseño por defecto se desincentiva o dificulta la protección de datos personales. (SERNAC, 2022, p.53)

"Patrón oscuro fuerte" o dark patterns (Control): *Es la combinación de la información sin consentimiento y el patrón oscuro de confirmación. En él no hay una solicitud expresa de consentimiento, sino que sólo se informa el uso de cookies en el sitio y el único botón es la aceptación de todas las cookies. No se informa la opción de configuración, sino que, en caso de querer configurar, los usuarios deben ingresar a un enlace a la política de privacidad (Figura 11). Una vez dentro de la política, al final de su texto, se entregó la opción de configurar cookies, las cuales por defecto tienen un formato de opt-out.* (SERNAC, 2022, p.53)

1.4 Diferencias entre las cookies y la memoria caché

Las cookies son un sistema de almacenamiento que tienen sus propias características y funciones, sin embargo, muchas veces se puede confundir con la memoria caché, dado que ambas son sistemas de almacenamiento de información. Sin perjuicio de lo anterior, no son lo mismo, y su principal diferencia radica en que tienen propósitos diferentes.

En el caso de una memoria caché, *está es una capa de almacenamiento de datos de alta velocidad que almacena un subconjunto de datos, normalmente transitorios, de modo que las solicitudes futuras de dichos datos se atienden con mayor rapidez que si se debe acceder a los datos desde la ubicación de almacenamiento principal* (Amazon, n.d.).

En cuanto a su finalidad, tienen por objeto aumentar la capacidad de recuperación de datos y aumentar la velocidad de respuesta ante una solicitud al ingresar a un sitio web cuya información sólo se encuentra de forma transitoria y que en algunos casos puede ser a largo plazo, además de ser almacenada en una memoria RAM o un software. Por otra parte, en el caso de las cookies, estás presentan distintas finalidades según el tipo de cookies, a modo de ejemplo, encontramos entre ellas a las cookies técnicas y de personalización, que como ha señalado la Universidad de Valencia : *se trata de cookies de uso interno para el funcionamiento de la web* (Universidad de Valencia, n.d.), permitiendo la recopilación de información para los fines que cada sitio web estime como necesarios o pertinentes.

1.5 La utilización de cookies por parte de organismos públicos

Como bien señalamos previamente, las cookies son pequeños fragmentos de texto que almacenan información en el navegador y su uso no se limita solamente al ámbito privado, sino que también a las Instituciones u organismos públicos. En este sentido, siguiendo lo señalado por

el Profesor Ignacio Michea, podemos entender que se habla de uso de estos dispositivos en el ámbito público cuando: *Nos referimos a la interacción que existe entre organismos o entidades estatales con nuestros datos, sea por medio de recolección, almacenamiento, procesamiento de tales datos personales* (Michea, 2022, p.517.)

Asimismo, de conformidad a lo dispuesto en el Art 19 N°4 de nuestra Constitución Política y a la ley 19.628 sobre Protección de Vida Privada, las instituciones u organismos públicos deben informar el tratamiento que realizan de los datos personales recopilados. De igual manera, la ley 20.285 denominada como "Ley de transparencia" señala en su Artículo primero: *La presente ley regula el principio de transparencia de la función pública, el derecho de acceso a la información de los órganos de la Administración del Estado, los procedimientos para el ejercicio del derecho y para su amparo, y las excepciones a la publicidad de la información* (Congreso Nacional, 2008). Esta ley tiene como finalidad permitir el derecho al acceso de información por cualquier medio publicitario, esto mediante el principio de transparencia ampliamente aplicado en los organismos e instituciones públicas, dicho principio resulta fundamental para conocer el uso que dan las instituciones públicas a la información que es proporcionada.

Además, en su artículo segundo, dicha ley nos señala las instituciones que se encuentran sujetos a este principio. En relación con esto, el Consejo para la Transparencia ha creado una serie de guías con la finalidad de establecer estándares para la protección de datos personales por parte de las instituciones públicas. Si bien, actualmente no contamos con una regulación pormenorizada en cuanto al uso de las cookies en los sitios pertenecientes al gobierno de Chile, si se cuenta con políticas de privacidad en la que en algunas oportunidades se señala la utilización de sus cookies, pero esto no es siempre así, dada su incorporación de manera generalizada.

Caso distinto es el del propio Consejo para la Transparencia, el cual cuenta con su propia política interna sobre el tratamiento que realizan de las cookies. Esta política de cookies nos señala que solo se utilizan cookies propias, de sesión y cuya finalidad es establecer estadísticas, incorporando también el tiempo de caducidad de estas. Dentro de esta política se le debe informar al usuario del tipo de almacenamiento que se hará de los datos que ingrese: *Solicitar acceso sobre los datos relativos a su persona, su procedencia y destinatario, el propósito del almacenamiento y la individualización de las personas u organismos a los cuales sus datos son transmitidos regularmente* (Consejo para la Transparencia, n.d.), siguiendo la guía Protección de Datos Personales para Instituciones Públicas (aplicable a todos órganos pertenecientes a la Administración del Estado), publicado en el Diario Oficial con fecha 7 de diciembre de 2020, donde se debe mantener la debida confidencialidad de los datos que se recaben y el usuario tiene la posibilidad de modificar o rechazar las cookies del sitio web del

Consejo para la transparencia, porque su fundamento es el consentimiento que debe tener el usuario otorgándole de esta manera todos los derechos que la ley señale, esto con la finalidad, por ejemplo, de solicitar la modificación de datos erróneos, información sobre cómo es utilizada la información proporcionada, solicitar la eliminación o bloqueo de los datos entregados, etc.

1.6 La utilización de cookies en redes sociales

Las principales redes sociales utilizan las cookies para distintos tipos de funciones o usos, estas se pueden configurar según nuestras preferencias, indicando cómo desactivarlas y su finalidad, esto cumpliendo sobre la base de una política de cookies en relación a la recopilación o almacenan de información de sus usuarios, ingresando por la opción en centros de ayuda. A continuación, nos referiremos a Facebook, Instagram y Twitter:

Instagram y su política de cookies nos señalan que: Usan cookies, píxeles, almacenamiento local y otras tecnologías similares para mostrarte contenido que te resulte pertinente, mejorar tu experiencia y proteger tanto Instagram como para sus usuarios. También pueden usar las tecnologías para recopilar información sobre cómo se usa el Servicio (por ejemplo, qué páginas se visitan con mayor frecuencia y si aparecen mensajes de error en páginas concretas). *Estas tecnologías nos permiten recordar opciones que has elegido (por ejemplo, tu nombre de usuario, tu idioma o la región en la que te encuentras) y adaptar nuestro Servicio para ofrecerte funciones y contenido mejorados. Estas cookies también se pueden usar para recordar cambios realizados en relación con el tamaño del texto, la fuente y otros elementos de las páginas que puedes personalizar* (Instagram, n.d.). Además de lo anterior, las cookies en Instagram cuentan con la opción de mostrar publicidad de sus colaboradores a los cuales denominan como "partners comerciales" y donde la información se puede compartir con organizaciones ajenas a Instagram con fines publicitarios, de marketing, estadísticos y de análisis e incluso proporcionando la ubicación de internet, sin mencionar que otro problema en sus políticas de cookies es no señalar el tiempo que permanecerán activas o su fecha de caducidad, por lo que solo se limitan a señalar las cookies que utilizan. Por último, es preciso señalar que Instagram sufrirá algunas modificaciones en sus políticas de cookies a partir del 12 de diciembre de 2023.

En el caso de Facebook, su funcionamiento es muy similar al de Instagram al pertenecer a la misma compañía (META), sin embargo, establece de manera más detallada los usos de las cookies en cuanto a: Autenticación; Seguridad e integridad de los sitios web y los productos; Publicidad, recomendaciones, insigths y medición; Servicios y funciones de los sitios web; Rendimiento; análisis y estudios; Sitios web y aplicaciones de terceros. A pesar de lo anterior, igualmente fue multada por Francia el 31 de diciembre de 2021 *En particular, el Supervisor francés observó que los sitios*

web facebook.com, google.fr y youtube.com ofrecen un botón que permite al usuario aceptar cookies de inmediato; pero sin ofrecer una solución equivalente (botón u otro) que permita al usuario de Internet rechazar fácilmente el depósito de estas cookies (CNIL, 2022).

En cuanto a Twitter, se señala que se utilizan las cookies y otras tecnologías similares, como píxeles o almacenamiento local, que brindan una experiencia mejor, más rápida y segura. *Las cookies también se utilizan para operar nuestros servicios, que incluyen nuestros sitios web, aplicaciones, APIs, píxeles, integradores de contenido y notificaciones de correo electrónico. Concretamente, Twitter utiliza estas tecnologías para: Mantener tu sesión abierta en Twitter; Ofrecer las características y funcionalidades de los servicios de Twitter; Guardar y respetar tus preferencias; Personalizar el contenido que ves; Protegerte contra el spam y abusos; Mostrarte anuncios que sean más relevantes; Proporcionar funciones de suscripción y distribuir determinados contenidos; Comprender cómo interactúas con nuestros servicios y dónde podemos mejorar.; Medir la eficacia de nuestra publicidad y marketing; Valorar el rendimiento de nuestros servicios e identificar errores y otros problemas de calidad; Recopilar los datos que se utilizan para el funcionamiento de nuestra actividad —desde la medición del tamaño de nuestra audiencia hasta la aplicación de las Reglas de Twitter*. (Twitter, n.d.). Algo fundamental de Twitter, de lo cual carecen Facebook e Instagram, es que establece un catálogo con todas las cookies que utilizan indicando: el nombre, su función, el controlador de esas cookies, la política de privacidad a que está sujeta y la web de dominio. Ejemplo: lscr, esta cookie se emplea para autenticación del administrador en Scroll, Twitter Intl Co, https://twitter.com/en/privacy .scroll.com

1.7 La utilización de las cookies por proveedores de tecnología

Las cookies son programadas con la finalidad de mejorar la experiencia de los usuarios al ingresar a distintos sitios web, lo cual no es una excepción para los mayores proveedores de tecnología del mundo como: Apple, Samsung y Google.

En Apple se señala que *Las cookies te permiten comprar mediante el carrito y personalizar los sitios, y a nosotros nos permiten saber qué páginas visitan los clientes. Nos ayudan a medir la eficacia de los anuncios y búsquedas, y nos dan información sobre el comportamiento de los usuarios, que utilizamos para mejorar nuestros productos y mensajes* (Apple, n.d.). Las cookies no solo permiten personalizar la experiencia de los usuarios a través del sitio, sino que permite también - como señala su página - realizar compras, pero realizando la advertencia de que al desactivar las cookies, esto puede significar no tener acceso a todos los servicios, suponiendo una limitación al acceso a la navegación libre. En este caso, lo experimenta el carrito de compra y el pago por internet, dejando en claro los efectos negativos de desactivar las cookies. Además, señalan que sus políticas de cookies cumplen con los estándares señalados por la Cámara de Comercio Internacional de Reino Unido y solo utilizan

cookies de carácter necesario, comportamiento y de funcionamiento. En relación con las cookies de comportamiento, se señala que la información recopilada es totalmente anónima y las cookies de funcionamiento no persiguen la actividad del usuario cuando navega fuera de los sitios de Apple.

Por otra parte, en el caso de Samsung, su política de cookies se determina en base a la empresa operadora, que en el caso de Chile sería de propiedad de Samsung Electronics y su última modificación de política de cookies se realizó el 1 diciembre de 2021. *Es importante que siempre verifique las actualizaciones de esta Política, ya que podemos cambiarla de vez en cuando para reflejar los cambios en nuestro uso de cookies* (Samsung, 2021). En su página, señalan que trabajan con terceros para entregar sus contenidos y publicidad y, además, incorporan el concepto de cookies flash que lo definen como: *Las cookies de Flash son un archivo de datos que los sitios web que visita pueden crear en su computadora. Se utilizan con mayor frecuencia para mejorar su experiencia de navegación web* (Samsung, 2021) pero realizando la advertencia en cuanto a que estas cookies presentan el problema de que no se pueden configurar o controlar con las herramientas dispuestas, sino que solo se puede acceder por medio de una configuración especial. *Sin embargo, estas tecnologías pueden hacer uso de diferentes partes de su dispositivo de las cookies estándar, por lo tanto, es posible que no pueda controlarlas con las herramientas y configuraciones estándar del navegador, ya que solo se puede acceder a ellas a través del Administrador de configuración de Flash Player on-line.*(Samsung, 2021). De esta manera, podemos denotar que existe un grave problema de información, porque existen configuraciones que no pueden desactivarse de manera sencilla por parte de los usuarios y accediendo a un sitio de terceros. Además, señala que *Samsung Electronics no es responsable de la configuración de su navegador.*(Samsung, 2021)

Google, por su parte, representa a una de las mayores empresas que han sido sancionadas por incumplimiento a las políticas de privacidad por parte de la Unión Europea en los últimos años, fundamentada debido la falta de información a los usuarios sobre el almacenamiento de cookies, además de no solicitar el consentimiento de los usuarios en relación a las cookies publicitarias y almacenar información a pesar que los usuarios desactivan la opción. Debido a este tipo de situaciones, fue multada por la CNIL (Commission Nationale de l'Informatique et des Libertés), quien es el encargado de la protección de datos en Francia: *En diciembre de 2021 la CNIL impuso una multa de 100 M€ a Google (Google LLC y Google Ireland Limited por haber incurrido en diversas conductas que transgreden el artículo 82 de la ley francesa de protección de datos, en relación con la Directiva ePrivacy* (CNIL, 2022). Esta conducta por parte de Google, se replicó nuevamente en enero de 2022, pero en esa oportunidad por la recolección de información por medio de avisos.

Al ingresar a sus políticas de cookies, ellos señalan cuánto tiempo dura el funcionamiento de determinadas cookies, por ejemplo: *Google usa la cookie "CONSENT", que tiene una duración de 2 años*

para almacenar el estado de un usuario respecto a sus elecciones de cookies. Además, señala que "*La principal cookie que utiliza Google Analytics es "_ga"* (nombre proporcionado por google) *que permite a los servicios distinguir a un visitante de otro y tiene una duración de 2 años. La utilizan todos los sitios en los que se implementa Google Analytics, incluidos los servicios de Google. Cada cookie "_ga" es exclusiva de una propiedad específica, así que no se puede utilizar para rastrear a un usuario o navegador en sitios web no relacionados"* (Google, n.d.). Además, google también utiliza cookies como:"__gads" que permite mostrar anuncios relacionados con google y "_gac_" que es utilizada para medir o calcular la actividad de los usuarios.

Google en su política de cookies no es específico en cuanto a todas las cookies que utiliza para su funcionamiento sino que solo se limita a señalar algunas y el periodo de tiempo de funcionamiento de las que considera más relevantes.

Capítulo II: Directrices generales OECD y principios generales sobre la protección de datos personales.

2.1 Directrices generales OCDE

La OCDE en materia de protección de datos personales, se ha ido desarrollando desde la década de los 80, dando énfasis a los problemas transfronterizos de los datos personales desde 1985 y buscando una serie de soluciones. De esta misma manera, se hizo en 1998 una Declaración ministerial sobre la protección de la privacidad de las redes globales, buscando reafirmar el compromiso que ya existía en ese momento con respecto a la protección de la privacidad en las redes globales.

Estas Directrices pretenden dar respuesta a un ambiente de seguridad cada vez más cambiante, a través de la promoción del desarrollo de una cultura de seguridad – esto es, centrándose en la seguridad del desarrollo de sistemas y redes de información, así como en la adopción de nuevas formas de pensamiento y comportamiento en el uso e interconexión de sistemas y redes de información. (OCDE, 2002, p.6). Por lo tanto, se busca con esto, sentar las bases de una toma conciencia por parte de los Estados frente a los riesgos de seguridad que implica el utilizar los sistemas o redes de información, previniendo de esta forma, situaciones de vulneración de seguridad frente a los datos personales y, en caso de que ocurra lo anterior, dicho vulneración sea detectadas de manera oportuna y que permita asumir las consecuencias por parte de aquellos que sean responsables y de esa manera, replanteando cómo entienden la cultura de la seguridad.

Es de esta manera que la OCDE sigue con su intención de plantear principios generales que sean adoptados por los países en los ámbitos de seguridad y orden público *"La Declaración de la OCDE sobre el acceso de los gobiernos a los datos personales en poder de entidades del sector privado busca reforzar la confianza en los flujos de datos transfronterizos —fundamentales para la transformación digital de la economía mundial—, clarificando el modo en que los organismos de seguridad nacional y las fuerzas del orden público pueden acceder a los datos personales en virtud de los marcos jurídicos existentes. La Declaración supone un importante compromiso político por parte de los 38 países de la OCDE y la Unión Europea que lo han firmado en el marco de la Conferencia Ministerial de Economía Digital de la OCDE de 2022. La Declaración está abierta a la adhesión de otros países"* (OECD, 2022)

En el caso de Chile, los principios planteados por la OCDE se encuentran implícito en la normativa relativa a tratamiento y protección de datos personales, donde podemos identificar se encuentran presentes los principios:

Responsabilidad: Sobre todo controlador de datos debe recaer la responsabilidad del cumplimiento de las medidas que hagan efectivos los principios señalados anteriormente.

Seguridad: Se emplearán salvaguardias razonables de seguridad para proteger los datos personales contra riesgos, tales como pérdida, acceso no autorizado, destrucción, uso, modificación o divulgación de los mismos.

Transparencia: Deberá existir una política general sobre transparencia en cuanto a evolución, prácticas y políticas relativas a datos personales. Se deberá contar con medios ágiles para determinar la existencia y la naturaleza de datos personales, el propósito principal para su uso y la identidad y lugar de residencia habitual de quien controla esos datos

calidad de los datos. Los datos personales deberán ser relevantes para el propósito de su uso y, en la medida de lo necesario para dicho propósito, exactos, completos y actuales. (OCDE, 2002, p.6)

Pero debemos considerar otros principios que son relevantes en nuestro ordenamiento y que desarrollaremos a continuación:

2.2 Principio de Consentimiento libre, informado e inequívoco.

"Respecto al consentimiento frente al tratamiento de datos, es necesario mencionar el art. 4 y el art 6 del reglamento – ya mencionados anteriormente- en el numeral 11 del art 4 se define que se entenderá por " consentimiento del interesado: toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le concierne" y luego, el artículo 6 en su numeral 1 letra a): " el tratamiento sólo será lícito si se cumple al menos una de las siguientes condiciones: a) El interesado dio su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos" (Michea, 2022*)* . En cuanto a este principio, el profesor Michea ha señalado que el consentimiento debe cumplir distintos requisitos para que pueda considerarse como una declaración afirmativa por parte del sujeto y estos serian que sea: A) libre, B) Especifica, C) Informada y D) Inequívoca.

A) libre: "*Significa que el interesado no puede ser obligado a otorgarlo; y que la prestación del servicio no puede supeditarse al mismo".* (Sanz, 2021). Por ejemplo: cuando al no aceptar las cookies la página no funciona o no permita al usuario el ingreso a dicha página

B) Específico: "*El consentimiento debe ser obtenido para cada una de las finalidades para las cuales los datos personales son recogidos. Es decir, no es posible la obtención de un consentimiento general*". (Sanz, 2021) Por ejemplo: El evitar aceptar las cookies de manera general e ir a configurarlas una por una.

C)Informado: Este es el caso aplicado por el RGPD de la Unión Europea en su artículo 13. *"El interesado debe ser informado según lo dispuesto por el artículo 13 RGPD. Entre otros: Finalidad del tratamiento, Responsable del tratamiento y Derechos y cómo ejercerlos"* (Sanz, 2021)

D) Inequívoco: "*La acción por la cual se otorga el consentimiento debe ser clara y manifiestamente afirmativa*". (Sanz, 2021). Para que sea inequívoco se debe realizar de forma escrita, en ningún caso de forma tácita aceptar que el usuario consiente en ello.

Por lo mismo, en la práctica nos señala que este consentimiento es inexistente o no existe, dado que, el sujeto se siente obligado a manifestar su voluntad de manera afirmativa, puesto que en el caso contrario, sufrirá las repercusiones que implica el no aceptar las cookies de la respectiva página web. Incluso, se recurre a mecanismos que obligan tácitamente al usuario a aceptar una configuración en la que no necesariamente está de acuerdo, como es el caso de las opciones por defecto que realizan las páginas.

2.3 Principio de autodeterminación informativa.

Este principio se incorpora a nuestro ordenamiento por parte de la jurisprudencia a través de la modificación realizada el año 2018 al Artículo 19 n°4 de nuestra la Constitución política de la República, siguiendo de esta manera a países como Alemania y España. *"Antes de este reconocimiento expreso, el derecho a la protección de datos personales se había entendido como parte del contenido iusfundamentalmente protegido del derecho al respeto y protección de la vida privada, establecido en el artículo 19 N° 4 de la Constitución. Así lo había argumentado la doctrina y la jurisprudencia mayoritaria. Pero hoy eso debe ser repensado a partir del reconocimiento explícito del derecho a la autodeterminación informativa como un derecho independiente del derecho a la vida privada, consagrado a partir de la reforma constitucional del 2018."* (Contreras, 2020, p.89). Para ello, se tomó como punto de partida el fallo efectuado por el Tribunal Constitucional Federal Alemán y la sentencia del Tribunal Constitucional español sobre el alcance del derecho a la protección de datos personales en la Constitución de 1978.

El derecho a la autodeterminación informada nació a partir de la sentencia del tribunal Constitucional Federal alemán el 15 de diciembre de 1983, como respuesta a la posibilidad del tratamiento masivo de datos. Con lo cual se marcó un hito en la defensa de los derechos de personas a preservar y proteger su vida privada.

El tribunal Constitucional Federal alemán configura en su sentencia, a partir del derecho general de la personalidad recogido en los artículos 1.1 y 2.1 de la ley fundamental de Bonn, la facultad del individuo, derivada de la autodeterminación, de decidir básicamente por sí mismo, cuándo y dentro de qué límites, procede revelar situaciones referentes a la vida propia. Con lo cual se reconoce un derecho que se le ha denominado autodeterminación informativa (Palma, 2016).

El propósito de este principio, radica principalmente en la protección de los datos con la utilización que se hizo de los mismos en lo relacionado al censo poblacional y de las profesiones de la época, esto mediante preguntas enfocadas no solo a la identificación de los sujetos, sino que también enfocadas a ámbitos como la religión y nacionalidad. Estas pueden resultar discriminatorias y vulnerar la posibilidad de desarrollo de la persona. En virtud de lo anterior, el principio de la autodeterminación del individuo fue entendido como la libertad de decisión sobre las acciones que realizan o no los sujetos.

Siguiendo la anterior, una Sentencia del Tribunal Constitucional español relativa al alcance del derecho a la protección de datos personales en la Constitución de 1978, señaló: *El Tribunal Constitucional se pronunció por primera vez sobre el alcance del derecho fundamental a la protección de datos personales en la sentencia 254/1993, de 20 de julio. En esta resolución afirma que el artículo 18.4 de la Constitución consagra un derecho fundamental autónomo y diferente del derecho a la intimidad; ya que, cuando el artículo 18.4 dispone que la Ley debe limitar el uso de la informática para garantizar la intimidad, el honor y el pleno ejercicio de los derechos de los ciudadanos, está incorporando "una nueva garantía constitucional, como forma de respuesta a una nueva forma de amenaza concreta a la dignidad y a los derechos de las personas (...) un instituto que es, en sí mismo, un derecho o libertad fundamental, el derecho a la libertad frente a las potenciales agresiones a la dignidad y a la libertad de la persona provenientes de un uso ilegítimo del tratamiento mecanizado de datos, lo que la Constitución llama "la informática"* (Garriga, 2016) . De esta manera, esta Sentencia no solo establece un derecho a la intimidad, sino que amplía el concepto a todos los datos personales, sin realizar una distinción si estos son privados o de público conocimiento.

En el caso de Chile, durante la discusión legislativa de este principio, se instauró un debate en cuanto a la posibilidad de consagrar expresamente el principio de la autodeterminación informativa, además de deliberar cuál sería la mejor vía para aplicar este principio, debatiéndose si sería por medio de la acción de protección o la acción de la Habeas data. Este proceso, finalizó con *el reconocimiento explícito de un nuevo derecho fundamental en la Constitución chilena requiere de una reconstrucción de su contenido, sentido y alcance respecto del legislador, en la eventual reforma a la Ley No. 19.628, y respecto los operadores jurídicos en la resolución de casos concretos* (Contreras, 2020, p.114). Finalmente, de las conclusiones que plantea el académico Pablo Contreras, podemos entender que este principio

actualmente se encuentra expresamente consagrado en el artículo 19 n°4 y que se puede recurrir tanto a la acción de Habeas data como a la acción de Protección.

En cuanto al Hábeas data, está es una figura que se puede interponer en los juzgados civiles o de letras (con competencia en lo civil) y consiste en *el procedimiento mediante el cual una persona puede requerir datos personales suyos que estén alojados en bases de datos, ya sean públicas o privadas*. (Poder Judicial, 2020). Esta acción, se centra en la eliminación de datos personales y la no entrega o difusión de los datos personales que puede tener una persona de terceros. Esto debe estar justificado y los magistrados deben evaluar las solicitudes, a su vez, si corresponde o no la entrega de datos.

2.4 Principio de neutralidad en la red o Acceso a la libertad de navegación web

En principio, el acceder a la información mediante la navegación web es más correctamente llamado como el principio de la Neutralidad en la red. De esta manera lo ha definido el Congreso Nacional a través del boletín 3915-19, señalando que este principio *asegura a todos los usuarios el acceso libre de contenidos o ejecutar aplicaciones o utilizar los dispositivos de su elección sin condicionamientos de ningún tipo. La "Neutralidad en la Red" consiste en que está en sí misma (no sus extremos) transmita toda información sin mirar ni jerarquizar y tampoco priorizar, con lo cual se asegura que la red es la misma para todos* (Congreso nacional, 2019*)*. Este principio, lo que busca es evitar el condicionamiento del acceso a la información de la navegación web, evitando de esta manera *condicionar el acceso de los usuarios de internet, discriminando contenido, aplicaciones o dispositivos* (Congreso nacional, 2019*) ,* por lo tanto, tiene un enfoque amplio evitando condicionar solamente a la web en sí misma, y al ser un concepto de amplio alcance *deja desatendido el problema de la concentra-ción de la propiedad en la Red, y por tanto el abuso de posición dominante, la mercantilización de los datos de los ciudadanos o el control sobre los mismos.* (Márquez, 2018) .

Con lo anterior, se busca evitar *"zero rating" (o tarifa cero) es una práctica comercial que revivió el debate sobre los alcances de la aplicación del principio de neutralidad de la red. Con ésta, los Proveedores de Servicios de Internet eximen al usuario final de la cobranza por tráfico de datos relativos a determinados sitios y aplicaciones de internet* (Rossini y Moore, 2015 citado por García, 2020). El Zero rating, implica la priorización de cierto contenido, aplicaciones o servicios, por sobre otros, lo que puede significar una discriminación en la búsqueda por parte de los usuarios. Estas colaboraciones con ciertos patrocinadores que en el último tiempo han implicado incluso un problema de seguridad, han enviado a los usuarios a páginas sugeridas que recolectan información (principalmente bancarias), un ejemplo de esto fue Banco Estado: *"la creación de una página web de similares características, colocándola dentro de los primeros resultados del buscador de Google"* (The Clinic, 2023). Lo anterior, implicó pérdidas

millonarias a microempresas y por esta razón, el Banco Estado decidió querellar por este phishing (ataque que roba dinero o la identidad de la persona).

Todo lo anterior, llevado a el paradigma de las cookies, implicaría que si se le diera un mayor énfasis al principio de neutralidad de la red como mecanismos regulador , evitando situaciones como los fraudes informáticos por medio -por ejemplo- de los patrocinios implementados por Google como sugerencia en la búsqueda del navegador o evitaría condicionar el acceso de los usuarios.

2.6 Sanciones aplicadas por órganos internacionales a la utilización de cookies.

Uno de los casos más controvertidos a nivel internacional fue la filtración de datos que sufrió la plataforma Yahoo! en el año 2014, pero del cual se tuvo conocimiento público posteriormente al ataque informático. Se señaló por parte de Yahoo! que: *Él a lo menos, 500 millones de cuentas y datos en línea de Yahoo, fueron robados de la compañía. Yahoo con posterioridad dio a conocer que los datos fueron accesados usando forged cookies, lo que permitió la filtración de la contraseña de cuenta y el acceso a los datos personales de millones de usuarios quienes utilizaban esta plataforma web. Los problemas no se agotan con lo anterior. Yahoo, nuevamente, el 2013 sufrió otra filtración de datos, basados en el mismo sistema de robo –las forged cookies – entregando la información personal de miles de usuarios que utilizaban su plataforma* (Michea, 2022, 511-512). Si bien, no se tuvo acceso a información en relación con datos bancarios, ésto sí afectó a: contraseñas encriptadas, preguntas y respuestas de seguridad, información de contacto de los usuarios, etc. Ante esta situación, la compañía se comprometió a mejorar su sistema de seguridad y realizó las respectivas sugerencias a sus usuarios, lo que fue de suma relevancia para tomar conciencia de la importancia de proteger los datos personales de los usuarios. Sumado a lo anterior, todo esto provocó que en ese momento la Unión Europea impusiera sanciones en el Reglamento General de Protección de Datos Personales (RGPD), todo esto, con la finalidad de proteger los datos personales y cuya implementación comenzó a partir de 2018.

Por lo anterior, las sanciones que se pueden determinar en este tipo de casos se han fortalecido y han aumentado, en ese sentido, a modo de ejemplo, se decidió aplicar multas por un porcentaje que toma en consideración el tamaño de la empresa, y las cuales pueden llegar hasta los 20 millones de euros. Sobre esto, "el *RGPD permite a las autoridades de protección de datos de cada país imponer sanciones y multas a las organizaciones que consideren infractoras. La sanción máxima es de 20 millones de euros o de 4% de los ingresos globales, lo que sea mayor. Las autoridades de protección de datos también pueden imponer sanciones, como prohibición de procesamiento de datos o amonestaciones públicas"* (Unión Europea, 2018)

Por otro lado, en el caso de EE.UU, específicamente en el Estado de California, desde el año 2020 se aprobó la Proposición número 24, la CPRA, agregando de esta manera, nuevas políticas en relación con la protección de la privacidad, así *"Las empresas sujetas a la CCPA tienen varias responsabilidades, incluida responder a las solicitudes de los consumidores para ejercer estos derechos y brindarles ciertos avisos que expliquen sus prácticas de privacidad . La CCPA se aplica a muchas empresas, incluidos los corredores de datos"* (Departamento de Justicia del Estado de California, n.d.). Lo anterior complementa al sistema existente de autorregulación de EE. UU.. Por tanto, en el Estado de California, las empresas deben informar sobre las cookies que se emplean y obtener el consentimiento, dado que cada error intencional podría implicar una multa de 7.500 dólares.

Luego, en el caso de Chile, el proyecto de ley sobre protección de datos personales - en actual tramitación - supone el establecimiento de sanciones claras para aquellas infracciones o incumplimientos que se realicen en la protección de los datos personales, estableciendo esto en base a la clasificación de leves, graves o gravísimas en su artículo 35.

2.7 Proyecto de ley "protección de datos personales" en relación con las cookies

Si bien, el proyecto de ley no contempla un artículo explícito que se refiere a las cookies, estas igualmente se pueden entender como incorporadas, esto dado el amplio ámbito de aplicación que este proyecto presenta. Igualmente, es posible que con la implementación de la Agencia de Protección de Datos Personales, por medio de sus respectivos reglamentos internos, la situación pueda cambiar y se establezcan disposiciones en relación a las cookies, como es el caso del Reglamento General de protección de datos de la Unión Europea que hace una mención expresa a modo ejemplar sobre las cookies como un identificador en su numeral 30 señalando: *"Las personas físicas pueden ser asociadas a identificadores en línea facilitados por sus dispositivos, aplicaciones, herramientas y protocolos, como direcciones de los protocolos de internet, identificadores de sesión en forma de «cookies» u otros identificadores, como etiquetas de identificación por radiofrecuencia. Esto puede dejar huellas que, en particular, al ser combinadas con identificadores únicos y otros datos recibidos por los servidores, pueden ser utilizadas para elaborar perfiles de las personas físicas e identificarlas"* (Comisión de Constitución, Legislación, Justicia y Reglamento, n.d.)

En el caso de España, se implementó una guía sobre el uso de las cookies por parte de la Agencia de Protección de Datos, lo más destacado de está guía es la "Responsabilidad de las partes en la utilización de las cookies". Destacando:

1. El editor o los terceros utiliza las cookies para finalidades exceptuadas de las obligaciones de informar y de obtener el consentimiento (Agencia Española de Protección de Datos, 2023, p.31). Se refiere al caso en que se requieran cookies por parte de terceros, estos deben ser solicitados con la finalidad de cumplir la prestación de servicios al usuario, pero el acuerdo se debe firmar directamente con las entidades, para que solo se utilice para la prestación de servicios señalada o en caso contrario se requerirá obtener el consentimiento del usuario. *2. El editor o los terceros utilizan las cookies para finalidades no exceptuadas de las obligaciones de informar y de obtener el consentimiento* (Agencia Española de Protección de Datos, 2023, p.31). De esta manera, se pueden utilizar cookies propias, pero existe de igual forma la obligación de informar y obtener el consentimiento, además, en el caso de cookies de tercero, se debe cumplir el garantizar que los usuarios estén informados sobre las cookies y las finalidades.

Sobre la situación anterior, la Agencia Española agrega: "*el nivel de responsabilidad de cada una de ellas deberá evaluarse caso por caso y teniendo en cuenta todas las circunstancias pertinentes en función de sus responsabilidades respectivas asumidas en la determinación de medios y fines del tratamiento".* (Agencia Española de Protección de Datos, 2023, p.32)

Capítulo III: Regulación de las cookies en nuestro ordenamiento jurídico y resguardo al Artículo 19 n°4 CPR

3.1 Ley N°19.628 sobre la protección de la vida privada.

La ley 19.628 se promulgó el año 1999, y con el paso del tiempo ha experimentado distintas modificaciones *(Ley 19.812, Ley 20.463, Ley 20.521 y Ley 20.575)* (Biblioteca Congreso Nacional, n.d.). La última de ellas fue la ley 21.504 la cual modificó el artículo 17 de la ley 19.628 enfocada a la prohibición de informar sobre deudas de prestación de servicios o acciones de salud. La ley ,en su inicio, se centró en el ámbito comercial, dando énfasis al tratamiento de datos en relación con prestaciones bancarias, posteriormente, esto se amplió a órganos públicos y privados para garantizar la protección de la vida privada consagrado en el Artículo 19 n°4 CPR.

Es así como la Ley 19.628 en su Artículo 4 se refiere al tratamiento de los datos personales, donde podemos señalar que: 1. Que sólo la ley o disposiciones legales lo pueden autorizar 2. El consentimiento del titular debe ser: informado, autorizado por escrito y debe contar con la posibilidad de ser revocada.

El problema se encuentra en el inciso quinto del Artículo 4 de la Ley 19628. Sobre esto, se ha señalado que *la implicancia de lo anterior es importante, ya que es la misma ley quien libera o crea una excepción para tales registros de exigir un el consentimiento expreso de una persona para que se realice el tratamiento de datos personales. Pero llama aún más la atención lo siguiente; tenemos una ley que otorga excepciones de requerir el consentimiento a personas jurídicas de carácter privado, y, además, es la misma ley la que permite que tal manejo de datos personales sea realizado no solo por tal entidad, sino que autoriza a entrar al uso de estos a entidades asociadas o aliadas a quien directamente obtiene esta información* (Michea, 2022, p.538). La norma en cuestión es contradictoria, por exigir el consentimiento expreso de la persona, pero por otra parte, permite que entidades con personalidad jurídica de carácter privado también tengan acceso a la información, lo que puede generar o derivar en su mal uso.

De igual manera, esta Ley se encuentra desactualizada frente a los desafíos sobre la evolución tecnológica y sobre el tema del almacenamiento de datos. Si bien, nuestra Constitución se refiere en su artículo 19 n°4 al tratamiento y protección de datos privados mediante una interpretación extensiva de la ley, debiendo ser resguardado, a su vez, por parte de órganos públicos, es el SERNAC (perteneciente al Ministerio de Economía) el encargado debe llevar a cabo la supervisión y fiscalización del cumplimiento de la protección de los datos personales, pero en la práctica su

potestad sancionatoria no ha sido suficiente y por lo mismo, los tribunales de justicia han conocido sobre estas causas, por medio de la acciones: habeas data y el recurso de protección.

También, debemos considerar que en relación al habeas data como acción jurisdiccional que en *nuestro país el control de la legalidad en el tratamiento de datos, se efectúa a posteriori por parte del titular de los datos ejerciendo los derechos que le concede la ley ante los responsables de los bancos de datos ya sean estos privados o públicos, o bien, ante los Tribunales de Justicia mediante el ejercicio por parte del afectado de la acción de habeas data que ha sido consagrada con rango legal en el artículo 16 de la Ley de Protección a la Vida Privada, a diferencia de la generalidad de los ordenamientos a nivel latinoamericano que tienen legislaciones protectoras de datos en donde se recibe reconocimiento constitucional a esta, como por ejemplo, Colombia, Perú, Paraguay, Argentina.* (Jervis, 2003)

3.3 Resguardo derecho fundamental a la protección de datos personales Art 19 N°4 CPR y Limitación o restricción al acceso a la información.

El artículo 19 n°4 CPR señala: *"El respeto y protección a la vida privada y a la honra de la persona y su familia, y asimismo, la protección de sus datos personales.* ***El tratamiento y protección de estos datos se efectuará en la forma y condiciones que determine la ley".***

Dicha norma, que surge producto de la modificación que sufre la ley 19.628 mediante la ley 21.096 en el año 2018, considerando expresamente el Derecho de protección de datos personales (también denominado autodeterminación informada), debiendo interpretarse de manera amplia esta protección de los datos personales, refiriéndose asimismo toda información personal, entre esto podemos señalar que *la protección de datos personales tiene por función garantizar a su titular "un 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* (Contreras, 2020, p.91)

Este derecho fundamental, sobre el tratamiento y protección de Datos Personales, por su parte, se ha visto mermado por las diversas formas de almacenamiento de datos que emplean tanto instituciones públicas como entidades privadas, a través de las cookies como forma más utilizada. Las cookies han generado distintas limitaciones por medio de: Las opiniones por defecto en opt-out y patrones oscuros o dark patterns.

De lo anterior, surge la denominada "paradoja de la privacidad". La cual consiste en una creación jurisprudencial que tiene como propósito buscar una explicación al comportamiento de los usuarios, en cuanto a sus afirmaciones las cuales, a su vez, difieren de su comportamiento. Podemos definir a esta última como: *La discrepancia entre la preocupación expresada y el comportamiento*

real de los usuarios, es decir, las personas afirman estar muy preocupados por su privacidad, pero hacen muy poco para proteger sus datos personales (SERNAC, 2022, p.15). Esto se ve estrechamente relacionado con los sesgos cognitivos, los cuales afectan la percepción de los usuarios en cuanto a la toma de decisiones lógica y racional, es decir, son *: errores sistemáticos en el proceso de toma de decisiones de las personas, que desvían su comportamiento de la lógica y racionalidad de un comportamiento deseable, afectando su proceso de decisión y aumentando su vulnerabilidad* (SERNAC, 2022, p.15). Entonces, el problema radica en cómo ingresa la información o se adquiere la misma, generando una percepción equívoca de los riesgos de la privacidad, sin tomar verdadera consciencia de las consecuencias que esta misma puede producir.

Por lo mismo, las cookies han significado un problema frecuente en este ámbito, al existir manipulación en las páginas web por medio de configuraciones que confunden al usuario que finalmente acepta sin entender con claridad los términos y condiciones impuestos. Entonces,*" las opiniones por defecto o respuestas preseleccionadas tienen un impacto muy significativo en la toma de decisiones de las personas, ya que éstas tienden a mantener la opción entregada por defecto y, por lo tanto, su decisión es influida por la arquitectura de decisión predefinida por el regulador o la industria"* (SERNAC, 2022, p.18).

Por lo tanto, la configuración por defecto nos lleva a la paradoja de la privacidad, dado que sirve como herramienta para manipular u orientar al comportamiento deseado por parte del programador, siendo posible una configuración por defecto que el usuario, para aceptar todas las cookies y para modificarlas, debe ir a la respectiva configuración.

A lo anterior, podemos agregar las denominadas *"dark patterns" (patrones oscuros) en el comercio electrónico. Los patrones oscuros se han definido como opciones de diseño presentes en las interfaces de sitios web o aplicaciones que dificultan la decisión de los consumidores, obligando o guiando a los usuarios para que tomen decisiones sub-óptimas para sus propios intereses. Ha esto también se le denomina como "sludge"* (SERNAC, 2022, p.19).

Al analizar en conjunto las "dark patterns" y las configuraciones por defecto activada para aceptar todas las cookies (opt-out) sin realizar una discriminación en cuanto a su relevancia, el SERNAC pudo identificar que existe un mayor nivel de aceptación de todas las cookies, siendo un 99.08% de la muestra realizada si sumamos ambos elementos versus el resto del porcentaje que fue inferior al 1% que rechazó todas las cookies o solo aceptó una o dos cookies adicionales. Entonces, las opt-out en conjunto con las dark patterns generan un problema grave de consentimiento real por parte de los usuarios, vulnerando de esta manera el Artículo 19 n °4 de la CPR y limitando el acceso a la información.

Esta situación se busca mejorar en el proyecto de ley que modifica la actual ley -que se encuentra aún en tramitación - con la incorporación de una agencia de Protección Datos Personales que busca asemejar al modelo planteado por España. Lo anterior, sería de suma relevancia puesto que "La Agencia Española de Protección de Datos (AEPD) es la autoridad estatal de control independiente encargada de velar por el cumplimiento de la normativa sobre protección de datos. Garantiza y tutela el derecho fundamental a la protección de datos de carácter personal de los ciudadanos" (Agencia Española de Protección de Datos, n.d.)

Capítulo IV: Las cookies y su relación con la IA, desafíos para el Derecho

4.1 Aplicación de Inteligencia Artificial (IA) a las cookies y su ayuda a la ciberseguridad.

La evolución y la globalización han influido en el nuevo contexto social que se experimenta sobre la tecnología, surgiendo una serie de desafíos que se presentan con la masificación al acceso a las Inteligencias Artificiales. Por esta misma razón la Unión Europea ha tomado medidas por la rápida expansión y magnitud de este fenómeno, y por lo mismo, han señalado que: *La tecnología permite que tanto las empresas privadas como las autoridades públicas utilicen datos personales en una escala sin precedentes a la hora de realizar sus actividades. Las personas físicas difunden un volumen cada vez mayor de información personal a escala mundial. La tecnología ha transformado tanto la economía como la vida social, y ha de facilitar aún más la libre circulación de datos personales dentro de la Unión y la transferencia a terceros países y organizaciones internacionales, garantizando al mismo tiempo un elevado nivel de protección de los datos personales* (Unión Europea, 2016)

Lo anterior, nos lleva a pensar en la estrecha relación existente entre las cookies y la Inteligencia Artificial, dado que ambas pueden colaborar entre sí y potenciarse, todo esto con el propósito de lograr un fortalecimiento en diversos aspectos asociados al almacenamiento de datos y ciberseguridad. De esta manera Inteligencias Artificiales como el Chat GPT, al cual le planteamos lo anterior, nos entrega una respuesta como la siguiente:

La relación entre la Inteligencia Artificial (IA) y las cookies está vinculada principalmente al uso de cookies en el contexto de la recopilación y análisis de datos para mejorar los sistemas de IA y personalizar la experiencia del usuario en línea (ChatGPT, n.d.).

Es así, que podemos señalar una serie de campos en los cuales ambas se relacionan tales como: En la recopilación de datos, el análisis y alimentación de la IA por medio de las cookies, las recomendaciones y toma de decisiones automáticas y la utilización para mejorar el marketing que las empresas implementan.

Con lo anterior, podemos decir que la Inteligencia Artificial se ha posicionado como una herramienta cuyo uso se sigue ampliando a distintos ámbitos de la vida cotidiana, pero su relación con el Derecho se sigue desarrollando, puesto que este último aún necesita incorporar políticas en relación con la protección de los datos personales, enfocada principalmente al *"Principio de neutralidad en la red*", esté que se ha visto mermado por la utilización de las cookies como principal herramienta para la recopilación de información.

Es así, que la Inteligencia Artificial puede resultar una ayuda en relación con la incorporación de información que realizan las distintas páginas web con sus respectivas cookies y funcionar a su vez como un sistema de seguridad para el usuario indicándose los posibles problemas de aceptar las cookies y realizar sugerencias para una que el usuario pueda tomar una mejor decisión. Es así que el GDPR de la Unión europea ha señalado en su numeral 39 que: *"Los datos personales deben tratarse de un modo que garantice una seguridad y confidencialidad adecuadas de los datos personales, inclusive para impedir el acceso o uso no autorizados de dichos datos y del equipo utilizado en el tratamiento."* (Unión Europea, 2016).

Por lo tanto, la Inteligencia Artificial puede ser clave para garantizar esta seguridad y confidencialidad que ha señalado la Unión Europea, y evitar así una acción aplazadas ante los problemas de privacidad que realizan las cookies, por lo que puede ser relevante incorporar a la inteligencia Artificial como un sistema de detección, aunque obviamente, teniendo acceso solo a la información de las cookies y no a información que pueda comprometer la seguridad de las distintas empresas e instituciones.

Ahora bien, lo anterior, igualmente puede resultar negativo si no se regula de manera certera y oportuna por el Derecho, dado que la Inteligencia Artificial puede utilizarse como un medio para la recopilación de datos sin el consentimiento de los usuarios, actuando como un posible sustituto de las cookies. Esto puede significar una relevante fuente de ayuda a las empresas e instituciones a la hora de realizar campañas mejor enfocadas a su público objetivo, en la atención personalizada a los usuarios, etc, pero esto implicaría a su vez, el compromiso de crear un mecanismos de protección para los usuarios, donde se les informe de la manera más completa y sencilla sobre la implicancia de incorporar la Inteligencia Artificial con su recopilación de información y que también, haya sanciones ante situaciones de incumplimiento, para evitar los problemas que se tienen actualmente con las cookies, pero que en el caso de la Inteligencia Artificial puede acarrear secuencias más desfavorables en la protección de los datos personales de los consumidores y usuarios, esto producto de su automatización y evolución constante que no se había previsto en su totalidad y donde, recién el Derecho está tomando medidas para mitigar los efectos que esta puede tener.

Es por todo lo señalado previamente que la Unión Europea ha comenzado a tomar medidas frente al avance de la Inteligencia Artificial y ha creado la primera Ley sobre Inteligencia Artificial entrando en vigor recién el año 2026 en su totalidad[1].

Conclusiones

1. En cuanto al tratamiento de los Datos Personales, nuestra legislación actual resulta insuficiente para las necesidades que surgen a partir de la utilización de las cookies en nuestro ordenamiento jurídico. Esto está fuertemente asociado con la protección de los datos y el avance tecnológico, lo que, a su vez, supone numerosos riesgos en cuanto al tratamiento que se le da a nuestra información personal. Reflejo de lo anterior, es que nuestro ordenamiento jurídico ha tenido que recurrir a la vía judicial para permitir un mayor resguardo Constitucional, por medio de el Habeas data y la Acción o Recurso de protección. En virtud de lo anterior, evidentemente nuestra legislación está obligada a ajustarse a los estándares internacionales que diversos Organismos Internacionales han planteado para el resguardo efectivo de los datos personales de las personas.

2. Sumado a lo anterior, nuestro ordenamiento jurídico nada dice de manera expresa respecto a las cookies por lo que solamente podemos inferir su respectiva protección y considerando además que las cookies no presentan sanciones específicas a su incumplimiento en el tratamiento que realizan de los datos personales, siendo imposible ejercer la potestad sancionatoria contra los órganos públicos y privados.

3. Que existen distintos tipos de cookies con finalidades diversas, siendo las cookies técnicas las cuales permiten el correcto funcionamiento de los sitios web. Pero además, existen cookies que significan un problema para la seguridad de la información dado que efectúan rastreos de la actividad del usuario y almacenan información de los mismos sin su debido consentimiento. Para ello, recurren a mecanismos como las opciones por efectos o "dark patterns", las cuales recopilan información del usuario lo que, a su vez, produce la "paradoja de la privacidad" en los consumidores o usuarios.

4. En relación con todo lo anterior, el principio de la neutralidad de la red es un pilar fundamental para lograr el objetivo de evitar que las cookies sean medios para restringir el

[1]https://elpais.com/tecnologia/2023-12-08/la-ue-aprueba-la-primera-ley-de-inteligencia-artificial-del-mundo.html

acceso a un determinado sitio web o información a cambio de la entrega de datos personales que incluso pueden ser clasificados como sensibles;

5. Por lo mismo, se espera que con la aprobación de proyecto legislativo sobre "Protección de Datos Personales", haya una serie de modificaciones significativas que impliquen efectivamente un mayor resguardo a los usuarios, para poder evitar situaciones de vulneración datos personales, y que, si ocurre lo anterior, dicho incumplimiento conlleve una serie de sanciones económicas a organismos públicos o privados que no cumplan los estándares establecidos.

6. Con el avance de la tecnología, las cookies se han visto estrechamente relacionadas con la Inteligencia Artificial. Esto último podría implicar un mejoramiento en los sistemas de seguridad de las cookies, ya que, de esta manera, se pueden utilizar para evitar situaciones como el robo de información que posee las cookies y a su vez, potenciando un funcionamiento más efectivo de recopilación de información y más seguro para los usuarios o consumidores.

7. Por último, con la creación e incorporación de la Agencia de datos personales se buscaría incorporar una serie de medidas que permitan un resguardo efectivo a la protección de los Datos Personales. De esta manera, Chile cumplirá con los compromisos internacionales en los cuales se ha suscrito, adecuando el ordenamiento a estos estándares, lo que incluso a futuro podría llevar a la dictación de una ley de políticas de cookies y otros identificadores.

Bibliografía

Agencia Española de Protección de Datos. (n.d.). Agencia Española de Protección de Datos | AEPD. from https://www.aepd.es/

Agencia Española de Protección de Datos. (2019). Marco de Actuación de Responsabilidad social de la AEPD. Agencia Española de Protección de Datos. from https://www.aepd.es/sites/default/files/2020-01/marco-actuacion-responsabilidad-social-AEPD.pdf

Agencia Española de Protección de Datos. (2023, Julio 11). *La AEPD actualiza su Guía sobre el uso de cookies para adaptarla a las nuevas directrices del Comité Europeo de Protección de Datos | AEPD*. Agencia Española de Protección de Datos. Retrieved December, 2023, from https://www.aepd.es/prensa-y-comunicacion/notas-de-prensa/aepd-actualiza-guia-cookies-para-adaptarla-a-nuevas-directrices-cepd

Amazon. (n.d.). Qué es el almacenamiento en caché y cómo funciona. AWS. Retrieved December, 2023, from https://aws.amazon.com/es/caching/

Apple. (n.d.). Información jurídica - Uso de cookies por parte de Apple. Apple. Retrieved December, 2023, from https://www.apple.com/es/legal/privacy/es/cookies/

Biblioteca Congreso Nacional. (n.d.). Ley Chile - Ley 19628 - Biblioteca del Congreso Nacional de Chile. BCN. Retrieved December, 2023, from https://www.bcn.cl/leychile/navegar?idNorma=141599

ChatGPT. (n.d.). ChatGPT. Retrieved December , 2023, from https://chat.openai.com/

CNIL. (2022, January 6). Cookies: GOOGLE fined 150 million euros. CNIL. Retrieved December 8, 2023, from https://www.cnil.fr/en/cookies-google-fined-150-million-euros

Comisión de Constitución, Legislación, Justicia y Reglamento. (n.d.). Chile. Honorable Cámara de Diputadas y Diputados - Chile. Retrieved December, 2023, from https://www.camara.cl/legislacion/comisiones/informes.aspx?prmID=3301

Congreso Nacional. (2008, Agosto 20). Ley 20285 - Biblioteca del Congreso Nacional de Chile. Ley Chile. from https://www.bcn.cl/leychile/navegar?idNorma=276363

Consejo para la Transparencia. (n.d.). Política de privacidad. Consejo para la Transparencia. Retrieved December, 2023, from https://www.consejotransparencia.cl/politica-de-privacidad/

Consejo para la Transparencia. (2022). GUIA PROTECCIÓN DATOS PERSONALES PARA INSTITUCIONES PÚBLICAS. Consejo para la Transparencia. Retrieved December, 2023, from https://www.consejotransparencia.cl/wp-content/uploads/instruccion/2022/10/Guia-proteccio%CC%81n-datos-personales-para-instituciones-pu%CC%81blicas-VF.-Agosto2022.-11.pdf

Contreras, P. (2020). El derecho a la protección de datos personales y el reconocimiento de la autodeterminación informativa en la Constitución chilena. ESTUDIOS CONSTITUCIONALES, 18(2), 34. https://www.scielo.cl/scielo.php?script=sci_arttext&pid=S0718-52002020000200087

Departamento de Justicia del Estado de California. (n.d.). State of California - Department of Justice - Office of the Attorney General. Retrieved December, 2023, from https://oag.ca.gov/

García, N. (2020, May 11). Principio de Neutralidad de la red y zero rating (tarifa cero). BCN. Retrieved December 11, 2023, from https://obtienearchivo.bcn.cl/obtienearchivo?id=repositorio/10221/28751/1/BCN_Neutralidad_de_la_Red_y_zero_rating_edPM.pdf

Garriga, A. (2016). El derecho a la protección de datos personales en la Jurisprudencia del Tribunal Constitucional. vLex. Retrieved December 8, 2023, from https://vlex.es/vid/derecho-proteccion-datos-personales-642494393

Google. (n.d.). Cómo utiliza Google las cookies – Privacidad y Condiciones. Retrieved December 8, 2023, from https://policies.google.com/technologies/cookies?hl=es

Instagram. (n.d.). Meta Cookies Policy. Instagram Help Center. Retrieved December, 2023, from https://privacycenter.instagram.com/policies/cookies/

Jervis, P. (2003). Derechos del Titular de Datos y Habeas data en la Ley 19.628. Retrieved December, 2023, from https://revistas.uchile.cl/index.php/RCHDI/article/view/10644

MAQUEO, M., MORENO, J., & RECIO, M. (2017, junio). Protección de datos personales, privacidad y vida privada: la inquietante búsqueda de un equilibrio global necesario. SciELO Chile. Retrieved December, 2023, from https://www.scielo.cl/scielo.php?script=sci_arttext&pid=S0718-09502017000100004

Márquez, J. J. (2018, noviembre 21). Vista de El principio de neutralidad en Internet. Una aportación a la libertad de comunicación en Internet desde el pensamiento de Francisco de Vitoria. Estudios de Deusto. Retrieved December, 2023, from https://revista-estudios.revistas.deusto.es/article/view/1522/1871

Michea, I. (2022). Derecho Informático: Capítulo I: La privacidad de datos personales en internet y las cookies. El jurista. https://vlex.cl/vid/capitulo-i-privacidad-datos-939672438

Michea, I. (2022). Derecho Informático: Capítulo III: La actual realidad nacional de las cookies con la ley Nº 19.628: un contraste frente a la realidad europea. El jurista. https://app-vlex-com.bibliotecadigital.uv.cl/#vid/capitulo-iii-actual-realidad-939672465

OCDE. (2002). Directrices de la OCDE para la Seguridad de sistemas y redes de información: Hacia una cultura de Seguridad, OECD. Retrieved December, 2023, from https://www.oecd.org/sti/ieconomy/34912912.pdf

OCDE (2002). Directrices de la OCDE sobre protección de la privacidad y flujos transfronterizos de datos personales

OECD. (2022, December 14). Adopción de un acuerdo histórico para salvaguardar la privacidad en el acceso a datos policiales y de seguridad nacional. OECD. Retrieved December, 2023, from https://www.oecd.org/newsroom/adopcion-de-un-acuerdo-historico-para-salvaguardar-la-privacidad-en-el-acceso-a-datos-policiales-y-de-seguridad-nacional.htm

Palma, P. (2016, Enero 28). Autodeterminación informativa nació de sentencia alemana. Derecho-Chile.cl. Retrieved December 8, 2023, from https://derecho-chile.cl/sentencia-de-15-de-diciembre-de-1983-del-tribunal-constitucional-federal-aleman-ley-del-censo-derecho-a-la-autodeterminacion/

Poder Judicial. (2020, January 24). *Reportaje Judicial: El recurso de habeas data y su aplicación en Chile | Poder Judicial.* Poder Judicial TV. Retrieved December, 2023, from https://www.poderjudicialtv.cl/programas/reportaje/reportaje-judicial-el-recurso-de-habeas-data-y-su-aplicacion-en-chile/

Consejo para la Transparencia. (2021, January 5). Consejo para la Transparencia, politíca de cookies, Retrieved December, 2023, from https://www.consejotransparencia.cl/privacidad_cookies/politica-de-cookies/

Radiografía del Comercio Electrónico. (2019, May 24). SERNAC. Retrieved December, 2023, from https://www.sernac.cl/portal/619/w3-article-56291.html

Samsung. (2021, Diciembre 1). Política de Cookies. Samsung. Retrieved December 8, 2023, from https://www.samsung.com/cl/info/privacy/cookies/

Sanz, I. (2021, November 23). La importancia de un consentimiento libre, específico e inequívoco. UBT Compliance. Retrieved December 11, 2023, from https://ubtcompliance.com/blog/la-importancia-de-un-consentimiento-libre-especifico-informado-e-inequivoco/

SERNAC. (2022, Marzo). Consentimiento en el uso de Cookies: Evidencia experimental sobre el impacto de la privacidad por defecto y los patrones oscuros en las decisiones de los consumidores.

Servicio Nacional del Consumidor. https://www.sernac.cl/portal/619/articles-64969_archivo_01.pdf

The Clinic. (2023, February 6). BancoEstado presentó querella por fraude con su página web. The Clinic. Retrieved December, 2023, from https://www.theclinic.cl/2023/02/06/bancoestado-querella-fraude-pagina-web/

Torija, M. (2021, January 20). Historia de la cookie, e iniciativas en el mundo post-cookie o "Cookieless" — PROGRAMMATIC SPAIN. PROGRAMMATIC SPAIN. Retrieved December, 2023, from https://www.programaticaly.com/nacho-carnes/historia-de-la-cookie-e-iniciativas-en-el-mundo-post-cookie-o-cookieless

Twitter. (n.d.). Cómo se utilizan las cookies en X | Ayuda de X. Twitter Help Center. Retrieved December, 2023, from https://help.twitter.com/es/rules-and-policies/x-cookies

Unión Europea. (2016, April 27). DOUE-L-2016-80807 Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y ... BOE.es. Retrieved December, 2023, from https://www.boe.es/buscar/doc.php?id=DOUE-L-2016-80807

Universidad de Valencia. (n.d.). *Clases de cookies*. Universitat de València. Retrieved December, 2023, from https://www.uv.es/uvweb/universidad/es/politica-privacidad/politica-cookies/clases-cookies-1285919089277.html

Unión Europea. (2018). Artículo 83 UE Reglamento general de protección de datos. Privacy/Privazy according to plan. Retrieved December, 2023, from https://www.privacy-regulation.eu/es/83.htm