TFM Iyari Hernández

por IYARI CHEZEL HERNÁNDEZ ÁLVAREZ

Fecha de entrega: 21-sep-2020 09:48a.m. (UTC+0200)

Identificador de la entrega: 1392702290

Nombre del archivo:
348195_IYARI_CHEZEL_HERNANDEZ_ALVAREZ_TFM_Iyari_Hernandez_2869624_451135133.pdf (1.35M)

Total de palabras: 28176

Total de caracteres: 150218

uc3m | Universidad Carlos III de Madrid

Máster Universitario Derecho de las Telecomunicaciones, Protección de Datos, Sociedad de la Información y Audiovisual

Curso académico 2019-2020

Trabajo Fin de Máster

"Informe para Netflix sobre medidas legales a establecer para limitar y perseguir los usos abusivos de su plataforma"

Iyari Chezel Hernández Álvarez

Tutor:

Agustín Eugenio Asís Roig

Madrid, 21 de septiembre de 2020

RESUMEN

Las cuentas compartidas representan un problema de uso abusivo a las plataformas *streaming* porque las empresas dejan de percibir ingresos, que ha ido creciendo y que resulta muy caro para seguir siendo ignorado.

Por lo anterior, en el presente informe jurídico se analizan las posibles soluciones que Netflix pudiese implementar para hacer cara a la problemática. Para ello, se analiza el contenido de los términos de uso tanto de Netflix como de otras plataformas *streaming*; las implicaciones jurídicas de las medidas que estas han implementado y las medidas que se han sugerido, pero que aún no se han implementado. Las medidas estudiadas en el presente informe son: cambio frecuente de contraseña, sistema de autenticación de doble factor, uso de sistemas biométricos, asociación a dispositivos específicos, uso de geolocalización, bloqueo basado en la dirección IP y uso de inteligencia artificial, aprendizaje automático y análisis de comportamiento.

Palabras clave: Netflix, cuentas compartidas, términos y condiciones, cambio frecuente de contraseña, autenticación de doble factor, sistemas biométricos, asociación a dispositivos específicos, geolocalización, bloqueo de dirección IP, inteligencia artificial, aprendizaje automático y análisis de comportamiento.

ABSTRACT

Shared accounts represent a problem of abusive use of streaming platforms because companies stop receiving income, which has been growing and is too expensive to continue to be ignored.

Therefore, this legal report analyzes the possible solutions that Netflix could implement to face the problem. For this, the content of the terms of use of both Netflix and other streaming platforms is analyzed; the legal implications of the measures they have implemented and the measures that have been suggested, but have not yet been implemented. The measures studied in this report are: frequent password change, two-factor authentication system, use of biometric systems, association with specific devices, use of geolocation, blocking based on IP address and use of artificial intelligence, machine learning and behavior analysis.

Keywords: Netflix, shared accounts, terms and conditions, frequent password change, two-factor authentication, biometric systems, association to specific devices, geolocation, IP address blocking, artificial intelligence, machine learning and behavior analysis.

ABREVIATURAS

2FA	Autenticación de doble factor
AP	Audiencia Provincial
B2C	Business to consumer (*Negocio a consumidor*)
CEO	Chief Executive Officer (*Oficial Ejecutivo en Jefe*)
ISP	Proveedor de Servicios de Internet
LOPJ	Ley Orgánica del Poder Judicial
LPI	Ley de Propiedad Intelectual
LSSI	Ley de Servicios de Sociedad de la Información
OTT	Over The Top
RGPD	Reglamento General de Protección de Datos
STS	Sentencia del Tribunal Supremo
SVOD	Subscription Video On Demand (*Subscripción de video bajo demanda*)
TJUE	Tribunal de Justicia de la Unión Europea
UE	Unión Europea

ÍNDICE

ANEXO 1: Procedimiento para entablar una demanda vía civil en contra de un usuario.

ANEXO 2: Procedimiento en caso de existir una violación a la seguridad de los datos personales.

ANEXO 3: Medidas que se deben de tomar para el uso de datos biométricos.

ANEXO 4: Ciclo genérico para realización de Evaluación de Impacto.

ANEXO 5: Obligaciones y medidas a tomar en cuenta para el uso de inteligencia artificial, aprendizaje automático y análisis de comportamiento.

1. INTRODUCCIÓN

La empresa Netflix International B.V. solicita mis servicios jurídicos para analizar las medidas legales que debería tomar para limitar y perseguir los usos abusivos de su plataforma, específicamente, las cuentas compartidas a la luz de las violaciones a sus términos de uso, limitando su estudio al marco del Derecho Español. Si bien la empresa cuenta con otros problemas como infracciones a los derechos de propiedad intelectual por terceros, comúnmente llamados "piratería", se hace hincapié en que este no es objeto de análisis del encargo. Por lo tanto, en primer lugar, se analizará brevemente la naturaleza de Netflix y su modelo de negocio —solo para efectos académicos del presente Trabajo de Fin de Máster—, para así poder entender y estudiar mejor cuál es el alcance de la problemática que tiene la empresa, en qué consiste y cómo ha impactado en sus finanzas.

En el siguiente capítulo, se analizan las ventajas de la compartición de cuentas, seguido del análisis de los términos de uso de Netflix con el objeto de estudiar lo que contemplan, para así entender y analizar el escenario actual de las medidas tomadas sobre el asunto, cómo está regulado actualmente de cara a los usuarios, conocer sus implicaciones y deficiencias y, de esta forma, saber a mayor detalle cuáles son las infracciones en las que incurren los usuarios y analizar si pudiesen modificarse o no las cláusulas.

Posteriormente, se analizarán los términos y condiciones, así como las medidas que han tomado otras plataformas de la misma naturaleza de Netflix y que también tienen el mismo problema de la compartición de cuentas, con el objeto de analizar si han tomado o no medidas de cara al problema. Derivado de lo anterior, se expone una serie de posibles soluciones que se han planteado los especialistas y que Netflix podría implementar para tratar de reducir la tasa de compartición de cuentas; se explica cada una de ellas, y se hace un análisis jurídico acerca de los riesgos que conllevan y las medidas a contemplar en caso de llevar alguna posible solución a la práctica.

Por último, y derivado del análisis se emiten las conclusiones recomendaciones jurídicas a título personal acerca de las medidas y/o cambios que debería de realizar Netflix al respecto, de cara al problema que enfrenta actualmente, haciendo hincapié en que dichas medidas no van a erradicar por completo el problema porque es algo que inevitablemente seguirá subsistiendo, pero que pretenden reducir el problema en la medida de lo posible.

2. ANÁLISIS DE LA PROBLEMÁTICA

2.1. Descripción de Netflix

Netflix es una plataforma *Over The Top*[1] (en adelante "OTT") de SVOD (*Susbscription Video On Demand*) que ofrece a sus usuarios un acceso ilimitado a un catálogo muy vasto de obras audiovisuales, tales como películas, series y documentales que pueden ser vistos vía *streaming* donde quieran, cuando quieran y desde cualquier dispositivo que cuente con acceso a internet, a cambio del pago de una tarifa plana mensual.

El éxito de Netflix radica en que supo entender la convergencia en el ámbito de las comunicaciones audiovisuales[2], pues propició el terreno ideal para que los servicios de televisión, cine e Internet funcionaran de manera adecuada y coordinada; siguiendo un modelo de negocio basado en la personalización del servicio, la ausencia de publicidad o tenedor libre —que ha ocasionado el fenómeno de *binge watching*, que consiste en consumir una serie por tres o más horas seguidas[3]—, el sistema de recomendaciones, la producción de contenidos propios, *long tail*[4] y la descarga de contenidos. Esto ha convertido a Netflix en la plataforma OTT audiovisual más importante en el mundo, con presencia en más de 190 países.[5]

Elaboración propia

2.2. ¿Cuál es la situación del abuso por parte de los usuarios?

Resulta cada vez más habitual el abuso por parte de los usuarios de Netflix a sus términos de uso[6]. Específicamente, el problema radica en que estos comparten sus contraseñas con

---

[1] Término que se traduce literalmente como "excesivo", pero aplicado al contexto de las tecnologías de la comunicación puede traducirse como "de transmisión libre", el cual no tiene una definición unánime, pero que se puede decir que son aquellas plataformas que hacen uso de Internet para ofrecer sus servicios de audio y/o video (específicamente hablando de las plataformas audiovisuales como Netflix), sin la intervención de un operador de telecomunicaciones, y que es posible gracias a la neutralidad de la red.

[2] HEREDIA RUIZ V., (2016), Revolución Netflix: desafíos para la industria audiovisual, *Chasqui, Revista Latinoamericana de Comunicación*, No. 135, pág. 284.

[3] SIRI L., (2016), El rol de Netflix en el ecosistema de medios y telecomunicaciones: ¿El fin de la televisión y del cine?, *Hipertextos*, Vol. 4, No. 5, pág. 58.

[4] Término acuñado por Chris Anderson en su artículo "The Long Tail", publicado en 2004 en la revista *Wired*, que se puede consultar en https://www.wired.com/2004/10/tail/, y que es mencionado por NEIRA E., (2018), Impacto del modelo de Netflix en el consumo cultural en pantallas, *Anuario AC/E 2018 de cultura digital,* Acción Cultural Española, pág. 73.

[5] https://help.netflix.com/es-es/node/412

[6] https://help.netflix.com/legal/termsofuse

otras personas, tales como familiares, amigos, parejas e incluso exparejas o simplemente personas que se unen para pagar una sola suscripción y resulte más barato. Esta práctica es muy común y vulnera específicamente las cláusulas 4.2 y 5 de dichos términos de uso, que señalan que el acceso al contenido es de uso personal y no puede ser compartido con terceros ajenos a la suscripción.

Al respecto, cabe mencionar que, por lo general, hay dos formas de compartir contraseñas:[7]

a. Casual. Se comparte con familiares y/o amigos, es aceptado ampliamente y no tiene ánimo de lucro. Bien puede compartirse de forma gratuita o mediante una cooperación entre los miembros para que entre todos se pague el costo total de la suscripción mensual.
b. Fraudulenta. Se comparte con miles de personas, tiene ánimo de lucro y generalmente el fin es malicioso. Esta práctica constituye un delito contra la propiedad intelectual, tipificado en el artículo 270 apartados 1 y 2 del Código Penal. No obstante, no es objeto de estudio del presente documento.

Por otro lado, si bien la misma empresa ofrece tres planes de suscripción distintos[8] donde permite que el usuario pueda acceder a la plataforma y ver el contenido hasta en cuatro dispositivos a la vez, esto deja entrever que sí es posible compartir la contraseña con más personas, incluso así lo han señalado expresamente los ejecutivos de Netflix en distintas entrevistas que se les ha hecho, ya que ellos mismos consideran que este es un fenómeno que les ha permitido captar un mayor número de clientes. No obstante, esta misma situación se vierte en su contra, ya que los usuarios se saltan el vacío que hay en los Términos de Uso de Netflix y comparten contraseñas en circunstancias distintas a las que la empresa había previsto originalmente, lo que ha ocasionado que Netflix deje de percibir los ingresos que se habían fijado en las metas iniciales.

Al respecto, cabe mencionar que, en 2016, Reed Hastings, CEO de Netflix, declaró que la compartición de contraseñas no era un problema, pues "*nos encanta que las personas*

[7] https://www.synamedia.com/video-solutions/video-security/credentials-sharing/
[8] https://www.netflix.com/signup/planform

En 2018, Netflix dejó de percibir más de 135 millones de dólares mensuales debido a la compartición de cuentas.

compartan Netflix [...] es algo positivo, no negativo"[9]. No obstante, la situación fue empeorando y actualmente sí es un problema ya que, de conformidad con los datos que arrojó un estudio realizado por la consultora Magid para la CNBC[10], en 2018 Netflix dejó de percibir poco más de 135 millones de dólares al mes, debido a que aproximadamente un 10% de sus usuarios comparte contraseñas con otras personas ajenas al círculo familiar, siendo una práctica muy común especialmente en los jóvenes, pues de ese porcentaje, el 35% pertenece a la generación de los *millenials*, mientras que el 19% corresponde a la *generación X* y el 13% a los *baby boomers*. Esta situación también fue confirmada por una encuesta realizada por Reuters[11] en junio de 2019, en donde los resultados arrojados indican que las personas de 18 a 24 años son las que más tienden a pedir prestadas contraseñas para acceder a los servicios de Netflix y demás plataformas. Es decir, se trata de un problema generacional, principalmente.

Las personas que más comparten cuentas son los millenials y los baby boomers.

Esto se traduce en millones de dólares de ingresos potenciales que Netflix está dejando de percibir, tal y como se señala en el estudio de Magid. Incluso, el 16 de octubre de 2019, en el informe de ganancias obtenidas en el tercer trimestre de dicho año, Spencer Neumann, director financiero, comentó que ya se encuentran monitoreando la compartición de cuentas y están trabajando en las medidas que van a tomar el respecto, y que se estudiará alguna manera amable con el consumidor, pero que no había nada decidido por el momento[12].

---

[9] TECH EVENTS, 07 de enero 2016, CES 2016 Netflix Press Conference Reed Hastings Keynote (P1). [Archivo de video]. Recuperado de: https://www.youtube.com/watch?v=XCdrx9TDEaE

[10] SALINAS S., (19 de agosto, 2018), Millennials are going to extreme lengths to share streaming passwords, and companies are missing out on millions, *CNBC*, Recuperado de: https://www.cnbc.com/2018/08/19/millennials-are-going-to-extreme-lengths-to-share-streaming-passwords-.html

[11] WEBER M., (Junio, 2019), Can I have your password?, *Reuters*. Recuperado de: http://fingfx.thomsonreuters.com/gfx/rngs/USA-TELEVISION-PASSWORDS-POLL/010041YS48H/index.html

[12] NETFLIX INVESTOR RELATIONS (16 octubre, 2019), *Netflix Q3 2019 Earnings Interview* [Archivo de video], Recuperado de https://www.youtube.com/watch?v=NHK51RgeqdY&feature=youtu.be&t=1825

Por su parte, la agencia Parks Associate publicó un estudio[13] en el que se revela que para 2021, el problema de las cuentas compartidas va a generar unas pérdidas de hasta 9.9 mil millones de dólares para las plataformas de video, así como una pérdida de 1.200 millones de dólares. Por esta razón, es que esta problemática no se puede tomar a la ligera y seguir permitiendo deliberadamente como hasta el día de hoy.

Si bien en su más reciente informe del primer trimestre de 2020 de fecha 21 de abril de 2020[14], Netflix tuvo un incremento de casi 16 millones de suscriptores y triplicaron sus ganancias con respecto al 2019, generando 709 millones de dólares entre enero y marzo del mismo año y ya no hicieron mención alguna acerca del problema de la compartición de cuentas, cabe destacar que los mismos directivos son conscientes que estos resultados se debieron a la pandemia del COVID-19, donde una gran cantidad de países emitió medidas de confinamiento forzado, lo que provocó que muchas personas se unieran a la plataforma para sobrellevar la situación. Además, también influyó que Netflix se ahorró los gastos de campañas publicitarias debido a esa situación. Asimismo, los directivos estiman que el número de suscriptores se irá reduciendo en la medida en la que los países levanten el confinamiento y también debido a la crisis económica a la que se van a enfrentar algunos de ellos, según lo han señalado diversos economistas a nivel mundial.

3. ANÁLISIS DEL CONTENIDO

3.1. ¿Cuáles son las ventajas de la compartición de cuentas?

Hasta ahora, Netflix no ha hecho nada para frenar el problema de la compartición de cuentas e incluso, como se expuso en el epígrafe anterior, los directivos han señalado que no es un problema como tal, a sabiendas de que se trata de una práctica generalizada que viola los términos de uso. No obstante, Netflix nunca ha aplicado estas reglas. Esto se debe gracias a que esto se considera una excelente forma de marketing, pues así Netflix tiene una oportunidad para adquirir nuevos clientes ya que, a nivel de mercadotecnia, y basado en la ideología *sharing is caring*, no es

La compartición de cuentas tiene su origen en la economía colaborativa.

[13] PARKS ASSOCIATES, (15 de enero, 2020), Piracy and account sharing cost US pay-TV and OTT operators more than $9 billion in 2019 and forecasted to reach $66 billion worldwide by 2022. Recuperado de: https://www.parksassociates.com/blog/article/pr-01152020

[14] https://s22.q4cdn.com/959853165/files/doc_financials/2020/q1/FINAL-Q1-20-Shareholder-Letter.pdf

necesariamente una pérdida de ingresos,[15] sino que se relaciona con la economía colaborativa, como se conoce en España, o *sharing economy* como se le conoce internacionalmente.

La economía colaborativa surge gracias a la tecnología, específicamente, de Internet, que es el elemento central, pues permite aumentar exponencialmente la manera de compartir entre diversas personas un producto o un servicio, como el presente caso, a costos más bajos, y desarrollan mercados multilaterales que, a su vez, generan efectos de red. Otro rasgo de la economía colaborativa aplicable a Netflix, mas no definitorio, es la contratación bajo demanda en tiempo real. Por lo tanto, se define como un "*modelo de organización industrial en el que una plataforma electrónica facilita la contratación de servicios, [...] ofertados por un grupo de usuarios y demandados por otro grupo de usuarios*".[16]

El sistema *streaming* es una forma de economía colaborativa, pues Netflix ofrece una variedad de obras audiovisuales a sus usuarios que pueden ver cuando, donde y como quieran, a cambio de una contraprestación mensual. Esto ha sido bastante atractivo y ha hecho que más personas se sumen a la plataforma, gracias al efecto de red. Para ello, es necesario mantener los precios de la suscripción al nivel que podrían pagar los que visualizan Netflix, pero que no son los titulares de la cuenta como tal, es decir, mantener los precios bajos, pues si estos se elevan, lo que ocasionaría es que se correría el riesgo de que tanto estos como los suscriptores de retiren y acudan con los competidores.[17]

No obstante, es importante apuntar que Netflix nació con la idea de economía colaborativa vía *streaming*, pero actualmente ha variado un poco el modelo, no por Netflix, sino por los usuarios. Esto es así porque Netflix no presta un servicio de mediación entre los usuarios, como lo hace Uber, sino que el fenómeno de la compartición de cuentas surgió como una necesidad ajena a Netflix para que las personas se ahorraran el costo total de una suscripción mensual, y así entre todos disfruten del servicio pagando

---

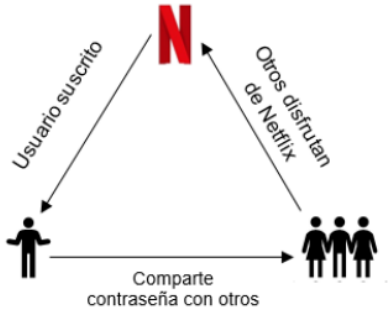
[15] SOUTHARD L., (28 de enero, 2020), Could streaming giants start to clamp down on password sharing?, *Marketplace*. Recuperado de: https://www.marketplace.org/2020/01/28/could-streaming-giants-start-to-clamp-down-on-password-sharing/

[16] MONTERO PASCUAL J.J., (2017), La regulación de la economía colaborativa, En Montero Pascual J.J. (Coord.), *La regulación de la economía colaborativa*, Tirant Lo Blanch, Valencia, pág. 23.

[17] SORIA BARTOLOMÉ B., (2017), Aspectos económicos de la economía colaborativa, *Op. Cit.*, pág. 62.

menos. De esta manera, se facilita la contratación temporal de los servicios, algo conocido como consumo colaborativo[18].

Es por ello, que el CEO de Netflix, Reed Hastings ha declarado que "*compartir contraseñas es algo con lo que tienes que aprender a vivir porque hay muchas comparticiones de contraseñas legítimas"*. Para el servicio de Netflix, esto queda expresado de la siguiente forma:



Elaboración propia

Ahora bien, ¿cuáles son estas comparticiones de contraseñas legítimas? que, dicho sea de paso y adelantando lo establecido en el capítulo siguiente, no están señaladas en los términos de uso. Al respecto, es menester señalar que, si bien estas prácticas legítimas no se encuentran literalmente en los términos de uso, sí fue posible localizarlas gracias a que los directivos de Netflix han señalado de forma informal en diversas conferencias las maneras en las que los usuarios tienen permitido compartir sus contraseñas, las cuales son las siguientes:

a. Entre los miembros de la familia (esposos e/o hijos) que viven en el mismo hogar. Esto es importante para los Directivos pues el hecho que los adultos compartan sus cuentas con los miembros más jóvenes de la familia los podría convertir en potenciales clientes a futuro.
b. Con los hijos, aunque no vivan en el mismo hogar que los padres. Netflix entiende que mientras los hijos estén en la etapa universitaria no cuentan con ingresos propios, en su mayoría, y siguen dependiendo de sus padres. No obstante, una vez graduados, esto los convierte en posibles usuarios independientes.

[18] VELASCO SAN PEDRO L. A., (2018), Economía colaborativa, En Barrio Andrés, M. y Torregrosa Vázquez J. (Coord.), *Sociedad Digital y Derecho*, pág. 638.

c. Con las personas que viven en el mismo hogar, aunque no sean familiares. Toda vez que, en muchas ocasiones, la adquisición de la suscripción es a nivel doméstico, Netflix considera razonable que la cuenta se comparta dentro del hogar, limitando su uso únicamente a los residentes de ese mismo hogar.

Por lo anterior, Netflix creó el llamado coloquialmente "plan familiar" —que en realidad se trata del plan premium— así como la opción de la creación de los perfiles, para que cada persona que vea la plataforma tenga su propia experiencia. Destacando también que esto se creó pensando en los supuestos legítimos antes enlistados. Por lo tanto, las ventajas que representan la compartición de cuentas para Netflix serían las siguientes:

1. La compañía crece gracias a la gran cantidad de espectadores que tiene, lo que le permite convertirse en el proveedor de servicios de comunicación audiovisual líder en el mercado, como lo es actualmente.
2. Ofrece nuevos modelos de negocio. Como se señaló en el epígrafe 2.1, Netflix es atractivo para los usuarios porque converge televisión, cine e Internet en una misma plataforma, lo que le permitió abrir nuevos nichos de mercado.
3. Tiene acceso a los datos y a las preferencias de más usuarios, lo que permite mejorar el algoritmo de preferencias, ofreciendo una experiencia más personalizada.

3.2. ¿Qué dicen los términos de uso de Netflix?

Los usuarios que comparten su cuenta de Netflix lo que hacen es esquivar su modelo de negocio, que en principio estaba pensado en que cada hogar necesita su propia cuenta, de manera que pudiese compartirse entre los miembros de ese mismo hogar. Pero para esto, es necesario primeramente revisar qué dicen exactamente los términos de uso de Netflix, ya que los términos y condiciones de uso son de las cosas más importantes que debe tener una plataforma, ya que una redacción errónea o deficiente puede ocasionarle problemas a su titular.

Pero ¿qué son los términos de uso? Estos también son llamados términos y condiciones[19] y tienen por objeto *"controlar el comportamiento de los usuarios cuando usan los*

[19] La definición legal se encuentra en el artículo 1.1 de la Ley 7/1998, de 13 de abril, sobre condiciones generales de la contratación.

servicios"[20], y son los textos legales que contienen los elementos que dictan la relación entre el usuario y el proveedor del servicio, cuyo contenido es fijado unilateralmente por este último, de manera que el usuario se limita a aceptarlas o a rechazarlas en su totalidad, de conformidad con la fórmula *take it or leave it*, sin estar en una posición de discutirlas o negociarlas, más bien a una imposición unilateral. Es decir, se trata de un contrato electrónico[21] de tipo B2C[22], que está supeditado a las reglas del Código Civil, pero también a la legislación del consumidor[23], puesto que una de las partes funge como tal, de manera que sus reglas e interpretaciones son de carácter especial, así como a la normativa de la sociedad de la información.[24]

En este contrato, calificado como contratación a distancia, en el que se van a establecer las reglas que van a imperar entre la relación usuario-prestador, se señalan cuáles son las obligaciones del prestador del servicio y las del usuario[25], las condiciones del servicio y

la forma en la que se puede acceder y hacer uso de dicho servicio, sin que ninguna de las cláusulas sea negociable. En términos estándar, se trata de un contrato de adhesión de tipo consensual, de manera que, una vez que el usuario acepta los términos de uso, este expresa su conformidad con lo que ahí se establece, quedando perfeccionado el negocio jurídico[26] y adhiriéndose por completo a todo su contenido que, como se ha dicho, son de potestad exclusiva del prestador del servicio. En consecuencia, una vez aceptados estos términos, las partes quedan obligadas[27].

---

[20] RODRÍGUEZ DE LAS HERAS BALLEL T., (Julio, 2009), Terms of Use, Browse-wrap Agreements and Technological Architecture: Spotting Possible Sources of Unconscionability in the Digital Era, *Contratto e impresa. Europa*, vol. 14, pág. 854.

[21] Es un contrato electrónico de conformidad con lo establecido en la letra h del Anexo de la LSSI, toda vez que la aceptación y la oferta de los Términos de Uso se realiza mediante equipos conectados a Internet que permiten el tratamiento y almacenamiento de datos y, evidentemente, esta se realiza a distancia.

[22] *Business to consumer*, es decir, entre el empresario y el consumidor.

[23] Las normativa aplicable es la Ley 7/1998, de 13 de abril, sobre condiciones generales de la contratación - tiene carácter imperativo, y es aplicable aún y cuando la empresa sea extranjera, pero el consentimiento se otorgó en territorio español, según su artículo 3°-; la LSSI; el Real Decreto Legislativo 1/2007, de 16 de noviembre, por el que se aprueba el texto refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias; y la Ley 3/2014, de 27 de marzo, por la que se modifica el texto refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias, aprobado por el Real Decreto Legislativo 1/2007, de 16 de noviembre.

[24] Artículo 23.1.II de la LSSI.

[25] Llamado consumidor y usuario de conformidad con el artículo 3 del Real Decreto Legislativo 1/2007, de 16 de noviembre, por el que se aprueba el texto refundido de la Ley General para la Defensa de los Consumidores y Usuarios

[26] Artículo 1262 del Código Civil.

[27] Artículo 1091 del Código Civil, en relación con el artículo 23 de la LSSI

Por lo tanto, es importante que estos términos sean redactados de forma muy clara, de manera que no haya lugar a dudas porque hay que recordar que el usuario promedio no es perito en la materia, por lo que el lenguaje a utilizar debe ser el más claro y simple posible, sin dar lugar a ambigüedades, especialmente, en aquellas cláusulas en las que se determinan las obligaciones para las partes. Esto es muy importante pues evita problemas a futuro, especialmente al momento de resolver el contrato ya que, si los términos incumplidos por el usuario no son claros y visibles, no es procedente[28]. A continuación, se exponen los puntos más importantes de los términos de uso de Netflix, relacionados con los problemas de cuentas compartidas.

En primer lugar, en la cláusula 4.2[29] se señala que los servicios contratados son para uso personal y no comercializable, además, no se pueden compartir con individuos fuera del hogar. Por su parte, la cláusula 5[30] indica que el titular de la cuenta es el responsable del control de esta y está obligado a evitar que terceras personas accedan a ellas, así como a no revelar su contraseña.

El servicio de Netflix únicamente se puede compartir entre las personas que vivan en el mismo hogar.

Haciendo una interpretación armónica de ambos artículos, se entiende que, si bien la suscripción es personal y el titular debe de evitar compartirla con otras personas, la excepción a la regla es que únicamente podrá compartirse la cuenta entre las personas que vivan en el mismo hogar, sin importar si son familia o amigos, basta con que vivan juntos, pero sin tener que acreditarlo. En caso de infringir estas

[28] Tribunal del Distrito de California, Sentencia de 17 de octubre de 2000, Pollstar vs Gigmania, Expediente CIV-F-00-5671 REC SMS.

[29] "*El servicio Netflix y todos los contenidos que se vean a través del servicio son para tu uso personal y no comercializable y no se pueden compartir con individuos fuera de tu hogar. Durante tu suscripción a Netflix, te concedemos un derecho limitado, no exclusivo e intransferible, para acceder al servicio Netflix y ver contenidos de Netflix. A excepción de lo mencionado, no se te transferirá ningún derecho, título o beneficio. Aceptas no utilizar el servicio para exhibiciones públicas.*"

[30] "*Contraseñas y acceso a la cuenta. El suscriptor que haya creado la cuenta de Netflix y cuyo Método de pago sea cargado (el "Titular de la cuenta") tiene acceso a la cuenta de Netflix y control sobre ella así como de los dispositivos compatibles con Netflix utilizados para acceder a nuestro servicio, y es responsable de la actividad que se realice en dicha cuenta de Netflix. Para mantener el control sobre la cuenta y evitar que cualquiera acceda a ella (que incluiría información sobre el historial de visionado de la cuenta), el Titular de la cuenta deberá mantener el control de todos los dispositivos compatibles con Netflix que se usen para acceder al servicio y no revelar a nadie ni la contraseña ni los detalles del Método de pago asociados a dicha cuenta. Eres responsable de actualizar y mantener la veracidad de la información que nos facilites acerca de tu cuenta. Podemos cancelar tu cuenta o bloquearla para protegerte a ti, a Netflix o a nuestros asociados de usurpación de identidad o de otra actividad fraudulenta.*"

cláusulas, la sanción que impone Netflix es que la cuenta podrá ser cancelada o bloqueada, es decir, se resuelve el contrato.

Por otra parte, la cláusula 4.3[31] indica que, dependiendo del plan contratado, será el número de dispositivos permitidos para ver el contenido simultáneamente. Es menester indicar que el plan básico permite visualizar una pantalla; el plan estándar, 2; y el plan premium, 4[32].

Del análisis de los términos de uso, se advierte que las formas permitidas para compartir contraseñas no son claras. Si bien los términos de uso dicen una cosa, los directivos de Netflix, en foros no oficiales señalan otra, por lo que se sugiere que estas formas permitidas queden incluidas expresamente en los términos de uso sin dejar lugar a dudas, de tal manera que se propone que se agregue una cláusula 5.1, cuya redacción que se propone es la siguiente:

> **5.1.** El Titular de la cuenta únicamente podrá compartir contraseñas con terceras personas en los siguientes casos:
>
> a. Entre las personas que vivan en el mismo hogar, sin importar si son o no familiares, siempre y cuando residan en el mismo lugar.
> b. Los padres podrán compartir su cuenta con sus hijos, aunque estos no residan en el mismo lugar que sus padres. Fuera de este caso, Netflix tiene terminantemente prohibido a los suscriptores que compartan sus cuentas y contraseñas con personas que no vivan en el mismo hogar.
>
> En caso de que Netflix detecte que un Titular de la cuenta ha compartido su usuario y contraseña en supuestos distintos a los aquí permitidos, la cuenta será cancelada de forma inmediata.

3.3. ¿Cuáles son las infracciones en las que incurren los usuarios?

De conformidad con el epígrafe anterior, la compartición de cuentas, en supuestos distintos a los establecidos en los Términos de Uso, viola el contrato. En la legislación española, esto se considera incumplimiento de contrato, vulnerando el principio de

[31] "*Puedes ver el contenido de Netflix principalmente dentro del país en el que hayas establecido tu cuenta y solo en las ubicaciones geográficas donde ofrezcamos nuestro servicio y hayamos licenciado dichos contenidos. El contenido disponible para visionado varía en función de la ubicación geográfica y cambia periódicamente. El número de dispositivos en los que puedes ver contenidos de forma simultánea depende de tu plan de suscripción y está especificado en la página "Cuenta"*."

[32] https://www.netflix.com/signup/planform

obligatoriedad[33] el cual dicta que *los pactos son para cumplirse*, pues los contratos tienen fuerza de ley y deben de cumplirse por ambas partes.

Además, *"los contratos se perfeccionan por el mero consentimiento"*[34], quedando las partes obligadas a lo pactado y a las consecuencias de ello. Por lo tanto, al estar expresamente señalado en los términos de uso que la compartición de cuentas fuera de los supuestos permitidos está prohibida, el usuario se encontraría incumpliendo dicha cláusula. Como consecuencia, hay dos posibilidades[35]: i) solicitar que se cumpla el contrato; o ii) solicitar su resolución más el pago de daños y perjuicios junto con los intereses.

Después de haber infringido los términos y condiciones por compartir la cuenta en supuestos no autorizados, a Netflix no le interesa solicitar que el usuario cumpla y se mantenga con el contrato, lo que le interesa a Netflix es que se resuelva el contrato y se le pague por los daños causados. No obstante, no se sugiere iniciar un proceso judicial en contra del usuario, sino simplemente resolver el contrato, ya que, lejos de incentivar a que más personas se suscriban, esto va a asustar y a alejar a los usuarios y a los posibles usuarios. Además, esto conllevaría consecuencias reputacionales negativas.

Por otro lado, cabe hacer dos precisiones. La primera de ellas es que hasta la fecha no ha habido ningún caso en el mundo en el que una plataforma de la naturaleza de Netflix haya interpuesto una demanda en contra de un usuario por compartir contraseña. No obstante, si Netflix decidiese iniciar un proceso judicial en contra de algún usuario que haya compartido indebidamente su cuenta, se debe de seguir el procedimiento establecido en el Anexo 1. La segunda precisión, consiste en que hay que tomar en cuenta que la resolución de un contrato por incumplimiento a los términos de uso no resuelve por sí el problema de los daños derivados a causa de la infracción de derechos de propiedad intelectual de las obras que, como se indicó al inicio, no es la cuestión por resolver en el presente documento.

Por otra parte, cabe destacar también que, ni en España ni en otro país de la Unión Europea, esta acción es considerada un delito, por lo que no es posible proceder por la vía penal, a diferencia de lo que ocurre en Estados Unidos, concretamente, en el Estado de

[33] Artículo 1091 del Código Civil.
[34] Artículo 1258 del Código Civil.
[35] Artículo 1124 del Código Civil.

Tennessee, en donde a través de la Ley Tennessee se criminaliza el intercambio de contraseñas en plataformas y servicios de suscripción de entretenimiento como Netflix, cuya pena va desde una multa por 2.500 dólares americanos y/o un año en la cárcel.

Conforme a la legislación española, la compartición de cuentas no es un delito y solo procede la resolución del contrato.

Asimismo, en Estados Unidos el intercambio de contraseñas es un delito federal en virtud de la Ley de Abuso y Fraude Informático (CFAA, por sus siglas en inglés)[36]. De conformidad con el caso Nosal, en el que son penalmente responsables tanto el usuario que comparte la contraseña, como el que accede a Netflix sin ser suscriptor y estar dentro de los supuestos de compartición legítima.

Es menester precisar que ambas leyes estadounidenses mencionadas lo consideran como delito en cuanto a la violación de la seguridad de los sistemas informáticos mas no en cuanto a materia de propiedad intelectual.

Por otro lado, sí cabe la existencia de una infracción extracontractual de los derechos de propiedad intelectual con los que cuenta Netflix, toda vez que, al compartir la contraseña en formas no autorizadas por Netflix, tanto el usuario que la comparte como el que goza de ella incurren en una infracción. Esto es así porque el usuario está posibilitando la reproducción a personas no autorizadas; entendiendo por reproducción en el sentido de poner una obra protegida en Internet a disposición del público[37], vulnerando el artículo 17 en relación con el artículo 18, ambos de la Ley de Propiedad Intelectual.

Esto es así porque Netflix celebra licencias con los titulares de las obras audiovisuales, en donde estos autorizan a Netflix a reproducir, distribuir y realizar comunicación pública de dichas obras para sus usuarios, no para terceros ajenos que se encuentren en situaciones no permitidas por Netflix, una de las razones por las cuales prohíbe la compartición de contraseñas, de manera que ambas personas son responsables de la infracción, pues

[36] Así lo determinó el 05 de julio de 2016 el Tribunal de Apelaciones del Noveno Circuito en el fallo del asunto Estados Unidos vs Nosal, en el que David Nosal le pidió a un empleado que compartiera sus credenciales con los demás para acceder a los registros de Korn/Ferry. Si bien se trata de credenciales para acceder a la base de datos de una empresa y no se dice expresamente que la compartición de contraseñas de Netflix es ilegal, los jueces en Estados Unidos han hecho una interpretación extensiva del fallo para aplicarlo también a plataformas como Netflix.

[37] BERCOVITZ ÁLVAREZ G., (2019), Los derechos de explotación. En Bercovitz Rodríguez-Cano R., *Manual de Propiedad Intelectual*, Tirant Lo Blanch, pág. 84.

conocen que la conducta infringe los términos y condiciones, además de que el usuario está cooperando para proveer los medios para que el otro acceda a la plataforma. Por lo tanto, en caso de querer proceder en contra del usuario y el tercero por infracción a la propiedad intelectual, se sugiere realizar el siguiente procedimiento:

1. Una vez que Netflix ha detectado la infracción y a los infractores, se sugiere que contacte vía correo electrónico al usuario para informarle la situación y solicitar que ponga fin a sus actos ya que, de lo contrario, se procederá por la vía judicial reclamando el pago de una indemnización por los daños causados por existir culpa por parte de los infractores.
2. Si el usuario en cuestión no deja de realizar la conducta infractora, se debe entablar una demanda a través de los Juzgados Mercantiles[38] con sede en el lugar en el que se cometa la infracción[39], en la que se debe solicitar[40]:
    a. Cese de la actividad ilícita de los infractores. Esto supondrá solicitarles a los infractores que dejen de realizar las actividades infractoras, de manera que se resolverá el contrato del usuario infractor y se imposibilitará su acceso a la plataforma en un futuro[41].
    b. Indemnización por los daños causados[42]. Se sugiere que Netflix haga un peritaje para conocer el valor de las ganancias que ha dejado de obtener a causa de la conducta infractora. Dependiendo del caso en concreto, se puede cuantificar la indemnización de la siguiente forma:
        i. La pérdida de beneficios que haya sufrido Netflix y los beneficios que hayan obtenido los infractores. Esto se sugiere no solicitarlo en el caso de uso doméstico, pues no supone la obtención de lucro. Además, esta debe de fundarse sobre cantidades probadas y no hipotéticas ya que se exige que el daño sea real y efectivo.[43]
        ii. La cantidad que hubiese percibido Netflix en caso de que el infractor se hubiese suscrito. Es decir, pagar las suscripciones conforme a los

[38] Artículo 86 ter apartado 2, letra a de la LOPJ.
[39] Artículo 52.1.11 LEC en relación con el artículo 86 ter de la LOPJ.
[40] Artículo 138 de la LPI.
[41] Artículo 139.1.b de la LPI.
[42] Artículo 140 de la LPI.
[43] STS 1919/2013 de 22 de marzo de 2013.

meses que haya utilizado la plataforma, probando el valor que tiene la suscripción en el mercado.[44]

iii. En cualquiera de los dos casos se puede solicitar también los gastos de investigación que se hayan realizado.[45]

iv. Daño moral[46]. Es el resultado de un cálculo a tanto alzado atendiendo a las circunstancias de la infracción y la gravedad de la lesión.

c. Medidas cautelares. Tienen como objetivo de no afectar el procedimiento hasta que se dicte sentencia. La medida cautelar que se puede solicitar en este caso es la suspensión de la actividad[47], es decir, cancelar la cuenta al usuario y que el tercero deje de acceder a la plataforma. Para ello, se debe acreditar lo siguiente[48]:

i. Peligro de la mora procesal. Consiste en justificar que, de no adoptarse la medida, se pudiesen dar situaciones que dificulten la efectividad de la tutela hasta que se dicte la sentencia.

ii. Apariencia de buen derecho. Aquí se deben de presentar las pruebas que evidencien las conductas infractoras.

iii. Caución. Netflix debe ofrecer una caución por los daños y perjuicios que pudiesen ocasionar a los infractores las medidas cautelares en caso de que se desestime la demanda.

d. Publicación de la sentencia. Esto se deja a consideración de Netflix si lo solicita o no, considerando la reputación y que esto supondría algo muy mediático que pondría los focos en la empresa.

Se recalca que este procedimiento es civil puesto que, como ya se señaló anteriormente, no constituye un delito, sino que constituiría una mera infracción de propiedad intelectual. Además, no hay antecedentes de que ninguna otra plataforma de la misma o semejante naturaleza de Netflix haya llevado a cabo esta acción.

[44] AAPL 164/2012.
[45] 140.1 LPI y Sentencia del TJUE C-99/2015 de 17 de marzo de 2016
[46] Se puede solicitar en ambos casos, conforme a la Sentencia del TJUE C-99/2015 de 17 de marzo de 2016.
[47] Artículo 141.2 de la LPI.
[48] AP de Madrid AC 2016/80 de 24 de noviembre de 2015 y JUR 2016/154318 de 15 de abril de 2016.

4. MEDIDAS TOMADAS POR OTRAS PLATAFORMAS

Atendiendo a la duda de Netflix, de conformidad con la ya mencionada encuesta de Magid, Netflix no es la única plataforma *on demand* vía *streaming* que presenta este problema, también lo tienen las demás plataformas audiovisuales tales como HBO, Disney+ y Amazon Prime Video, e incluso Spotify, quienes están dejando de percibir millones de dólares gracias a la compartición de cuentas por parte de sus clientes. Por lo tanto, se responderá a las preguntas planteadas por el cliente: *¿cuáles son las medidas tomadas por otras plataformas y qué dicen sus términos y condiciones?*

Si bien los términos y condiciones deben establecerse conforme a las necesidades propias de cada prestador de servicio, es menester señalar que el análisis de sus condiciones es relevante puesto que se trata de plataformas que no solo son de la misma naturaleza que Netflix, sino que también se trata de su competencia directa. Por lo que es importante analizar los puntos positivos con los que cuentan, y que son amigables con los usuarios, para así adaptarlos a Netflix con el objetivo de reforzar la posición de este en el mercado y seguir siendo la plataforma preferente por el público; de esta forma, gana Netflix y gana la audiencia.

4.1. Apple TV

Al igual que Netflix, no ha desarrollado ningún mecanismo en particular. Además, sus términos y condiciones[49] son bastantes similares a Netflix. Expresamente permite la compartición de cuentas, pero solamente entre familiares, pudiendo compartirse máximo con 6 personas. En caso de incumplimiento o sospechas de que se está incumpliendo el contrato, Apple resolverá el contrato y/o cancelará el ID del usuario.

4.2. Amazon Prime Video

Las reglas de uso[50] de Prime Video no son muy claras. Al igual que Netflix, no cuenta con una medida sólida para combatir la compartición de cuentas, puesto que solo permite hasta tres transmisiones a la vez, pero una misma película o serie solo puede reproducirse en un solo dispositivo.

[49] https://www.apple.com/legal/internet-services/itunes/es/terms.html
[50] https://www.primevideo.com/help/ref=atv_hp_cnt?_encoding=UTF8&nodeId=202095500

A diferencia de Netflix y otras plataformas, no señala que el uso es personal ni prohíbe la compartición de cuentas, lo cual indica que sus condiciones son bastante deficientes y no son un buen modelo para ser considerado por Netflix.

4.3. Disney+

Actualmente, y conforme a su contrato de suscripción[51], Disney no cuenta con ningún mecanismo para evitar las cuentas compartidas. En su contrato solo permite que el contenido pueda visualizarse simultáneamente en 4 dispositivos, pero el costo es mucho menor que el de Netflix[52], siendo 6.99 euros al mes.

No obstante, aunque por el momento no ha tomado ninguna medida para evitar el problema de las cuentas compartidas, en agosto de 2019, Disney y Charter anunciaron[53] que van a trabajar en conjunto para tratar de combatir el problema de compartición de cuentas, el cual ellos consideran como *piratería*[54]. La estrategia por seguir consiste en monitorear las direcciones IP de los usuarios de Disney y así saber desde qué dispositivos se accede a la aplicación, compararla con la lista de los datos y las direcciones IP de los usuarios de Charter y así bloquear las direcciones IP que accedan a la plataforma sin ser usuarios de Disney.

4.4. HBO

Conforme a sus términos y condiciones[55], los datos de acceso al servicio son de uso personal y expresamente se prohíbe la utilización por terceros. El método que emplea para impedir la compartición de cuentas es la asociación a dispositivos específicos, establecida en su cláusula 5.5. En esta cláusula, HBO solo permite que se usen y se registren máximo cinco dispositivos; para poder añadir uno nuevo, hay que eliminar uno anterior. Además, solo permite que dos de los cinco dispositivos registrados visualicen el servicio simultáneamente. En caso de uso no autorizado del servicio o incumplimiento de

---

[51] https://www.disneyplus.com/es-es/legal/contrato-de-suscripci%C3%B3n

[52] El plan básico cuesta 7,99 euros; el estándar, 11,99; y el premium, 15,99 euros.

[53] BROOKIN J., (16 de octubre, 2019), Disney Is Finally Taking On Account Sharers, *Wired*. Recuperado de: https://www.wired.com/story/disney-streaming-account-sharing/.

[54] Coloquialmente, se ha referido así a los delitos relativos a la propiedad intelectual, específicamente a la reproducción, comercialización y/o difusión de obras sin contar con el consentimiento del titular de los derechos de dichas obras. Por lo tanto, es erróneo considerar que la compartición de cuentas encuadra con este delito. Por otra parte, Martínez del Peral Fontón la define como *"la reproducción ilícita y la subsecuente comercialización o difusión fraudulenta de las obras [...] La característica que realmente tipifica la piratería es el lucro, el beneficio comercial rápido e importante"*.

[55] https://es.hboespana.com/terms-and-conditions

los Términos y Condiciones la consecuencia es la resolución del contrato y no se le reembolsará al cliente ningún cargo que haya abonado.

4.5. PlayStation

A diferencia de Netflix, ellos cuentan con términos de uso del software, puesto que lo que se comparte con los usuarios es la licencia de un videojuego, no la prestación de un servicio de comunicación audiovisual. No obstante, vale la pena analizar sus términos de uso y el mecanismo que ellos tienen para evitar el uso de cuentas compartidas.

PlayStation tiene diferentes documentos: Términos de servicio[56], Términos del uso del Software[57] y Contrato de licencia de Software[58], en los que se prohíbe de forma expresa compartir datos de cuentas. En caso de incumplir con los términos y condiciones, PlayStation restablecerá la contraseña, detendrá o suspenderá la suscripción, suspenderá el acceso a sus productos, suspenderá la cuenta o entablará acciones legales.

Si bien sus términos de uso no hacen referencia acerca de las medidas implementadas para evitar la compartición de cuentas, la respuesta se encuentra en la página de preguntas frecuentes[59], en donde se deduce que el mecanismo que ellos emplean es la asociación a determinados dispositivos haciendo diferenciación por el tipo de servicio y el tipo de consola. A su vez, PlayStation diferencia por el tipo de consola con la que cuenta.

	Juegos	Video
PS4	Dos dispositivos, una cuenta principal y una cuenta secundaria.	Dos dispositivos, una cuenta principal y una cuenta secundaria.
PS3	Dos dispositivos	Un dispositivo
PSP	Dos dispositivos	Tres dispositivos

De esta manera, para poder jugar o ver un video en un dispositivo diferente, se tiene que desactivar un sistema de forma manual o vía remota, de lo contrario, el sistema no permitirá acceder a otro dispositivo que no esté activado en el sistema.

[56] http://legaldoc.dl.playstation.net/ps3-eula/psn/es_tosua_es.html
[57] https://www.playstation.com/es-es/legal/software-usage-terms/
[58] https://doc.dl.playstation.net/doc/ps4-eula/ps4_eula_es.html
[59] https://www.playstation.com/es-es/get-help/help-library/my-account/device-activation-deactivation/activating-a-playstation-4-system/

4.6. Spotify

Spotify hace uso de la geolocalización. Cuenta con dos opciones de servicio, el gratuito y el de suscripciones de pago. En el primero no se paga una tarifa mensual, pero sí aparecen anuncios y tiene un límite de canciones permitidas para saltar. En cambio, en el servicio de suscripciones de pago o "premium" no hay anuncios, se pueden saltar las canciones las veces que quiera y se pueden descargar canciones, álbumes o playlists para ser escuchadas sin conexión. A su vez, la opción Premium cuenta con 4 planes: Individual, Dúo, Familiar y Estudiantes.

El plan individual es para 1 cuenta; el dúo es para 2 cuentas, pero que vivan en el mismo domicilio; el plan familiar es para 6 cuentas que vivan en el mismo domicilio; y el plan estudiantes es para 1 cuenta. Al plan individual le rigen los términos y condiciones generales de Spotify, mientras que a los demás planes les rigen esos mismos términos y condiciones más los términos específicos por cada plan, mismos que se analizarán a continuación.

En cuanto a la compartición de cuentas, en los términos y condiciones no se señala expresamente que está prohibido compartirla, únicamente se dice que el titular de la cuenta es el responsable del uso que se le haga a su nombre de usuario y su contraseña. Por otra parte, señala que, en caso de incumplimiento del contrato, se suspenderá el acceso al servicio.

a. Plan Dúo[60] y Plan Familiar[61]

En estos planes cada uno ingresa de forma independiente a la plataforma y tiene su propio perfil. Como requisito, se establece que los titulares de ambas cuentas deben residir en el mismo domicilio, lo que tendrán que confirmar una vez que activen las cuentas. Además, se establece que de vez en cuando se les pedirá que confirmen su domicilio para verificar que cumplen con los requisitos exigidos. Para esto, Spotify obliga a dar permiso para la geolocalización, con el objeto de que la empresa compruebe si efectivamente se está usando la cuenta en el mismo sitio que el resto de la familia.

[60] https://www.spotify.com/es/legal/duo/
[61] https://www.spotify.com/es/legal/premium-family-terms/

Spotify señala tanto en los términos y condiciones propios de ambos planes, así como en su Política de Privacidad[62] que, para verificar que efectivamente viven en el mismo domicilio, utilizará la aplicación de Google Maps para localizar los dispositivos y verificar la dirección, con el objeto de que se cumplan los requisitos geográficos de estos planes.

A su vez, la dirección que los usuarios proporcionen se sujeta a los términos del servicio adicionales de Google Maps[63] y la Política de Privacidad de Google[64] por lo que, al usar estos dos planes, Google también obtiene información de los usuarios como nombre, número de teléfono, correo electrónico, geolocalización, los navegadores y los dispositivos que se usan para acceder a los servicios, información sobre la red móvil y la dirección IP. Para la información de la localización, Google utiliza GPS, dirección IP, datos del sensor del dispositivo, información sobre elementos cercanos al dispositivo y cookies.

Además, Spotify señala que, en caso de que los usuarios no cumplan con estos requisitos, se reserva el derecho de rescindir o suspender el acceso al servicio.

b. Plan Estudiantes[65]

Este va dirigido solo para estudiantes de escuelas de enseñanza superior que estén acreditadas. No obstante, no se señala en los términos y condiciones cuáles son estas escuelas acreditadas.

Para acreditar la calidad de estudiante se deben de proporcionar los siguientes datos: nombre, institución educativa, correo electrónico, fecha de nacimiento y cualquier otro documento que acredite al usuario como estudiante.

5. ANÁLISIS DE LAS POSIBLES SOLUCIONES

Hasta el día de hoy, Netflix no cuenta con los mecanismos para distinguir la diferencia cuando inicia sesión un suscriptor a cuando inicia sesión alguien a quien este le compartió su contraseña, pues no cuenta con un mecanismo de identificación de identidad, solo identifica que la contraseña ingresada es la correcta. La única forma que tiene para saber

[62] https://www.spotify.com/es/legal/privacy-policy/
[63] https://maps.google.com/help/terms_maps/
[64] https://policies.google.com/privacy
[65] https://www.spotify.com/es/legal/student-discount-terms-and-conditions/

esto es a través de la autenticación, pues de esta manera se determina que la persona que está teniendo actividad en Netflix es quien dice ser. A continuación, se analizan las posibles soluciones que se han planteado y que incluso ya han sido implementadas por otras plataformas, conforme al capítulo anterior.

5.1. Cambiar frecuentemente la contraseña

La forma más sencilla y extendida de proteger las cuentas es a través de las contraseñas. El usuario le dice al sistema quién es —se identifica—, mientras que la contraseña lo autentica —comprueba que es quien dice ser—.

Sin embargo, de conformidad con un estudio hecho en octubre de 2019 por Harris Poll en asociación con Google[66], solo el 34% de los encuestados[67] cambia sus contraseñas constantemente. Además, aun habiendo compartido la contraseña de sus cuentas con sus parejas, solo el 11% de los estadounidenses cambia sus contraseñas después de una ruptura amorosa.

El Instituto Nacional de Estándares y Tecnología (NIST, por sus siglas en inglés)[68] recomienda que el cambio de contraseñas se haga únicamente después de recibir una notificación de acceso no autorizada a la cuenta, cuando surja un incidente de seguridad y cuando se haya compartido la clave con alguien a quien ya no se le va a compartir más la cuenta. En estos casos, y en aras de tratar de incomodar al usuario lo menos posible, el mecanismo que se podría implementar es el siguiente:

- Que el sistema no acepte información personal como nombre, apellido, fecha de nacimiento del usuario o alguna palabra que aparezca en los diccionarios.
- Que sea obligatorio que incluya minúsculas, mayúsculas, números y un carácter especial.
- Longitud mínima de ocho caracteres.
- La nueva contraseña no debe relacionarse con la anterior.

---

[66] GOOGLE y HARRIS POLL, (Octubre, 2019), The United States of P@ssw0rd$. Recuperado de: https://storage.googleapis.com/gweb-uniblog-publish-prod/documents/PasswordCheckup-HarrisPoll-InfographicFINAL.pdf

[67] La encuesta fue realizada a 3.419 adultos mayores de 18 años con residencia en Estados Unidos de América.

[68] GRASSI P., GARCIA M. y FENTON J., (2017), Digital Identity Guidelines, *National Institute Of Standards and Technology*, NIST Special Publication 800-63-3. Recuperado de: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf

- Contar con un medidor de contraseña, que indique si la contraseña es débil, fuerte o muy fuerte. En caso de que la contraseña sea débil, que aparezca un cuadro en donde se señalen consejos para fortalecerla, por ejemplo, si la persona pone todos los números o los caracteres especiales, sugerirle que los ponga en medio.
- No usar contraseñas por defecto.

5.1.1. Desventajas[69]

- Cambiar frecuentemente la contraseña resulta molesto y es frustrante para el usuario tener que buscar una nueva contraseña y memorizarla otra vez.
- Al forzar a los usuarios a cambiar sus contraseñas cada cierto tiempo, a la larga ya no usan contraseñas efectivas y tienden a seleccionar contraseñas bastante débiles, comprometiendo la seguridad de la cuenta. Incluso, tienen un 46% más de posibilidades de que sean adivinadas.[70]
- A la larga, los usuarios crean patrones que pueden ser predecibles, puesto que usan básicamente la misma contraseña, pero solo le cambian pequeños detalles, como una letra por un carácter semejante o se invierte el orden.
- La gente no puede recordar todas sus contraseñas.
- El cambio de contraseña no detendrá que la siga compartiendo con otras personas, puesto que muy probablemente seguirá compartiéndola. Sin embargo, sí es una medida efectiva contra los hackers.

5.1.2. Implicaciones jurídicas

En caso de que Netflix haga estas implementaciones, se deben de tomar las medidas técnicas y organizativas óptimas para proteger el acceso al sistema y así evitar el procesamiento no autorizado[71], por lo que se debe de tomar en cuenta lo siguiente:

- El estado del desarrollo tecnológico.
- Los costos de la implementación.

---

[69] CRANOR L., (02 de marzo, 2016), Time to rethink mandatory password changes, *Federal Trade Commission*, Recuperado de: https://www.ftc.gov/news-events/blogs/techftc/2016/03/time-rethink-mandatory-password-changes

[70] PETERSON A., (02 de marzo, 2016), Why changing your password regularly may do more harm than good, *Washington Post*. Recuperado de: https://www.washingtonpost.com/news/the-switch/wp/2016/03/02/the-case-against-the-most-annoying-security-measure-virtually-every-workplace-uses/?arc404=true

[71] Si bien el RGPD no dice nada específico acerca de las contraseñas, es menester indicar tomar en consideración el principio de seguridad establecido en el artículo 5 del RGPD en relación con el artículo 32 de dicho ordenamiento.

- Propósito del procesamiento.
- Revisión periódica del sistema de contraseñas.
- Usar un algoritmo de hash adecuado y actualizado que ofrezca protección contra los hackers.
- No permitir texto sin formato.

Es importante mencionar que, en cualquier caso, las medidas adoptadas deben de siempre garantizar la seudonimización de los datos, la confidencialidad, la integridad, la disponibilidad y la resiliencia, la capacidad de restaurar la disponibilidad de los datos y su acceso. Asimismo, estas medidas deben de estar en constante evaluación, esto en relación con el principio de responsabilidad proactiva, que se refiere a que se cumple la normativa de protección de datos y que se pueda demostrar su efectivo cumplimiento.

El incumplimiento a estas obligaciones conlleva al pago de una multa de hasta 20 millones de euros o hasta el equivalente al 4% del volumen del negocio total anual global, lo que resulte mayor,[72] además de una indemnización a los usuarios por los daños y perjuicios materiales e inmateriales causados[73].

En caso de existir una violación a la seguridad de los datos personales, se debe de hacer el procedimiento[74] descrito en el Anexo 2. El incumplimiento a estas obligaciones conlleva al pago de una multa de hasta 10 millones de euros o hasta el equivalente al 2% del volumen del negocio total anual global, lo que resulte mayor.[75]

5.2. Sistema de autenticación de doble factor (2FA)

En un inicio, se creía que este sistema era innecesario e incómodo, y que solo bastaba con una simple contraseña. Con el tiempo, las empresas se han dado cuenta que esto no es así, ya que ha surgido la necesidad de fortalecer la seguridad de las cuentas y controlar los accesos, por lo que surgió el sistema 2FA o de dos factores.

Con la autenticación se determina que el usuario es quien dice ser. El sistema consiste en crear capas adicionales que no permiten ser penetradas por personas no autorizadas, en este caso, por personas ajenas al usuario, que complementan la utilización de una contraseña simple, pues tiene como objetivo de que acceda solamente la persona que sí

[72] Artículo 83.5.a del RGPD.
[73] Artículo 82 del RGPD.
[74] Artículos 33 y 34 del RGPD.
[75] Artículo 83.4.a del RGPD.

está autorizada por el sistema, de manera que se aporte no solo la contraseña, sino también más información.[76] Esto se realiza mediante la combinación de al menos dos de las siguientes categorías:

Elaboración propia

- Algo que el usuario sabe, que es su contraseña, una respuesta a una pregunta de seguridad o una clave enviada al correo electrónico o al teléfono móvil. (Factor de conocimiento).
- Algo que él tiene, como un token. (Factor de posesión).
- Algo que el usuario es, como un dato biométrico, una característica física del usuario, como su voz, su huella dactilar, el iris o el reconocimiento facial. (Factor inherente).

Aunque no son muy utilizadas, cabe destacar que también existen otras dos categorías más:

- El lugar donde está el usuario, como la geolocalización.
- Algo que el usuario hace, como los hábitos del usuario.

Es decir, se combinan dos o más credenciales para demostrar que el usuario es quien dice ser y no es un impostor, ya que en el primer tipo (SFA, por sus siglas en inglés) —algo que el usuario ya sabe, como la contraseña— es lo más básico y también es el más vulnerable, como se explicó en el epígrafe anterior. De esta manera, se forman las capas, pues si se penetra una de ellas, se tienen que romper más capas para que el tercero ajeno a la cuenta pueda alcanzar su objetivo. Lo más importante de todo esto es diseñar un flujo de seguridad que se adapte a la experiencia del usuario.

Fuente: INCIBE y AEPD

[76] OFICINA DE SEGURIDAD DEL INTERNAUTA, (27 de febrero, 2019), El factor de autenticación doble y múltiple. Recuperado de: https://www.osi.es/es/actualidad/blog/2019/02/27/el-factor-de-autenticacion-doble-y-multiple

No obstante, no se debe confundir con el sistema de dos pasos o 2SV, pues este consiste en proporcionar dos elementos que pueden pertenecer a la misma categoría, como una contraseña y una clave vía mensaje o llamada telefónica, por ejemplo, que son dos cosas que el usuario sabe.

En el caso del 2FA, se refuerza aún más la seguridad del sistema puesto que se combinan dos categorías diferentes, que pueden ser algo que el usuario sabe y algo que él tiene, como su contraseña y un token, por ejemplo. Incluso puede reforzarse aún más agregando algo que el usuario es, como un dato biométrico, convirtiéndose en una autenticación multifactor, y cuya vulneración es mucho más difícil. Sin embargo, para efectos del objetivo que busca Netflix, un token no es algo recomendado, pues no solo va a resultar molesto o incómodo para el usuario, sino que también implicaría una inversión muy grande para Netflix que, a consideración de la suscrita, no es necesaria.

Por otro lado, tampoco se recomienda el uso de mensajes vía SMS o correo electrónico pues estos pueden ser inseguros[77], ya que pueden ser fácilmente interceptados, ya sea porque el sistema de conexión SS7 es vulnerable a los ataques; o ya sea mediante la ingeniería social, los ciberatacantes pueden hacer que la operadora móvil redirija el número móvil. En su lugar, lo óptimo sería generar una contraseña de un solo tipo (*One Time Password,* OTP por sus siglas en inglés) o un código QR a través de la aplicación de Netflix.

La ventaja de la autenticación es que mitiga los ataques de fuerza bruta de los cibercriminales, protege a los usuarios de *phishing*[78] y de infecciones por malwares, así como ataques a los servidores de la plataforma.[79]

Las contraseñas habituales son bastante riesgosas, de manera que la autenticación de dos factores reduce las posibilidades ya sea de un robo de cuentas o de que un tercero distinto al usuario tenga acceso a la cuenta. Si un atacante tiene acceso a las credenciales, con el

---

[77] GRASSI P., FENTON J. y NEWTON E., (2017), Digital Identity Guidelines, *National Institute of Standards and Technology*, NIST Special Publication 800-63B, pp. 44 y 45. Recuperado de: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63b.pdf

[78] Envío de correos electrónicos por parte de ciberdelincuentes en el que se hacen pasar por entidades legítimas, tales como bancos u organismos públicos.

[79] ENJOY SAFER TECHNOLOGY, Guía de doble autenticación, pág. 5. Recuperado de: https://www.welivesecurity.com/wp-content/uploads/2014/01/guia-autenticacion-eset.pdf

sistema de dos factores, este no podrá acceder a la cuenta[80], pues dificulta el acceso por completo, toda vez que se necesita de un código, mismo que solo puede conocerse si se cuenta con el dispositivo móvil o el correo electrónico.

La desventaja es que usar el 2FA en exceso puede ser frustrante e incluso intrusivo para la experiencia del usuario, por lo que se requiere usarlo solo cuando exista la amenaza de un riesgo. De esta forma, el mecanismo de autenticación estará ahí latente, pero solo cuando sea necesario como, por ejemplo, cuando Netflix detecte actividad inusual del usuario.

5.2.1. Implicaciones jurídicas

En materia de protección de datos, estas las podemos englobar en dos rubros: seguridad de los datos y biometría[81].

A. Seguridad de los datos[82]

1. Implementar medidas técnicas y organizativas adecuadas[83] para impedir el acceso a los datos a terceros ajenos, así como en el epígrafe 5.1.2, esto con el objetivo de cumplir con el principio de responsabilidad proactiva, es decir, garantizar que se cumple con la normativa y demostrar tanto a los usuarios como a las autoridades su cumplimiento.
2. Seudonimizar y cifrar los datos personales, que se garantice la confidencialidad, la integridad y la disponibilidad de los datos en el sistema, que se evalúen periódicamente las medidas técnicas y organizativas implementadas, y que estas sean acordes con los riesgos. Esto significa que, en caso de que la seguridad se vea comprometida, Netflix tenga la capacidad de restaurar la disponibilidad y el

- Adoptar medidas técnicas y organizativas óptimas.
- Seudonimización y cifrado.
- Proteger los datos desde el diseño y por defecto.
- Minimizar los datos.

[80] Mary Landesman, investigadora de seguridad de Norse Security, citado por ROSENBLANTT S., (22 de octubre, 2015), How to set up two-factor authentication, *The Parallax*, recuperado de: https://the-parallax.com/2015/10/22/how-to-set-up-two-factor-authentication/.

[81] MCDOWELL B., (2019), Three ways in which GDPR impacts authentication, *Computer fraud and security*, pp. 9-12. Recuperado de: https://reader.elsevier.com/reader/sd/pii/S1361372319300193?token=BEFEAFAAFB3B4F7FF76163F79E17F30B95A4C3F8F0DA41E010C906D922287B163B8585D7B3F36E381C654DBB51CB151E.

[82] El objeto de la seguridad es garantizar la confidencialidad, la integridad y la disponibilidad de los datos de los usuarios.

[83] Considerando 78 del RGPD.

acceso por parte de los usuarios a sus datos personales. Todas estas medidas deben verse reflejadas en todo el ciclo de vida de los datos.

3. Implementar las medidas desde el diseño y por defecto[84], tomando en cuenta el estado de la técnica, el coste de la aplicación, la naturaleza y los fines del tratamiento, en aras de garantizar que solo se utilicen los datos personales que realmente sean necesarios para su fin.
4. Atendiendo al principio de minimización de los datos[85], si se implementa este mecanismo, es importante que los datos deben ser adecuados, pertinentes y limitados a los fines necesarios. Este debe evaluarse cuantitativa y cualitativamente, es decir, atendiendo al tipo y cantidad de datos a tratar. Además, únicamente deben conservarse para el fin en específico.

Asimismo, en caso de que exista una violación a la seguridad de los datos, se debe seguir el procedimiento descrito en el Anexo 2, ya que de lo contrario, Netflix sería acreedor al pago de una indemnización por daños y perjuicios causados a los usuarios.[86]

En caso de que no se tomen las medidas de seguridad adecuadas, las consecuencias podrían consistir en: daños y perjuicios para los usuarios en su información como en sus derechos, discriminación, usurpación de identidad, reversión no autorizada de la seudonimización, pérdidas financieras tanto para los usuarios como para Netflix y daño reputacional para Netflix[87]. Esta es considerada una infracción grave, que se castiga con el pago de una multa de hasta 20 millones de euros o hasta el equivalente al 4% del volumen del negocio total anual global, lo que resulte mayor[88] más el pago de daños y perjuicios ocasionados a los usuarios.

Por lo anterior, es que se sugiere que este mecanismo no se encuentre por defecto, sino que únicamente sea activado cuando salte alguna alarma en caso de intrusión a la cuenta por parte de terceros ajenos.

---

[84] Artículo 25 del RGPD.
[85] Contemplado en el artículo 5.1.c del RGPD y criterio establecido por el Tribunal Constitucional en la STC 297/1996.
[86] Artículo 82 del RGPD.
[87] Considerando 85 del RGPD.
[88] Artículo 83.5.a del RGPD.

5. Biometría

El nivel de impacto al usar datos biométricos es alto.

Para la autenticación biométrica se emplean técnicas matemáticas sobre los rasgos físicos de una persona para verificar que es quien dice ser. En aras de fortalecer la seguridad de los sistemas, muchas empresas están empleando la biometría en sus sistemas de autenticación. El uso de datos biométricos empleando el 2FA es una forma en la que Netflix puede estar seguro en un 96% que quien ingresa a la cuenta realmente es el suscriptor, pues revela más información acerca del usuario[89], pero también es la manera más intrusiva que tendría con sus usuarios.

Cabe destacar que los datos biométricos son datos sensibles toda vez que identifican de manera unívoca a una persona[90], por tratarse de su voz, de su cara, su iris o la huella dactilar. Actualmente, las aplicaciones usan mayormente la huella dactilar o el reconocimiento facial.

Se sugiere que se lleven a cabo las siguientes medidas, que se describen a mayor detalle en el Anexo 3:

1. Se aconseja que la coincidencia y el almacenamiento de los datos biométricos se quede en el dispositivo[91] bajo el control exclusivo de los usuarios[92].
2. Deber de información. Se le debe de informar a los usuarios su finalidad y el tiempo que se recabará la información.
3. Obtención de consentimiento del usuario. Es importante que, en caso de adoptar esta medida, se recabe el consentimiento del usuario de manera expresa para que se puedan tratar sus datos.

---

[89] AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, (2020), 14 equívocos con relación a la identificación y autenticación biométrica, pp. 1 y 2. Recuperado de: https://www.aepd.es/sites/default/files/2020-06/nota-equivocos-biometria.pdf

[90] Artículo 4.14 en relación con el artículo 9.1 del RGPD. Cabe destacar que si bien la AEPD considera en su informe 36/2020 que son datos sensibles aquellos que tienen el objeto de identificar a un sujeto (uno-varios), no así la autenticación (uno-a uno) también señala que es una cuestión compleja que se tiene que atender al caso concreto y en tanto no se pronuncie el Comité Europeo de Protección de Datos se debe de adoptar la interpretación más favorable para el afectado. Por esta razón, atendiendo a la protección de los usuarios es que se considera que sí serían datos sensibles.

[91] COMISIÓN NACIONAL DE INFORMÁTICA Y DE LAS LIBERTADES (CNIL), (2018), Biométrie dans les smartphones des particuliers: application du cadre de protection des données. Recuperado de: https://www.cnil.fr/fr/biometrie-dans-les-smartphones-des-particuliers-application-du-cadre-de-protection-des-donnees

[92] COMISIÓN NACIONAL DE INFORMÁTICA Y DE LAS LIBERTADES (CNIL), (2018), Biométrie à disposition de particuliers: quels sont les principes à respecter ?. Recuperado de: https://www.cnil.fr/fr/biometrie-disposition-de-particuliers-quels-sont-les-principes-respecter

4. Deber de confidencialidad. Durante todo el ciclo, aún después de que termine la relación con los clientes.
5. Nombrar un Delegado de Protección de Datos. Esto es así, ya que se tratan a gran escala datos personales.
6. Es necesario demostrar la responsabilidad proactiva desde el diseño y por defecto.
    a. Elaborar un Análisis de riesgos, en el muy probablemente resulte que el nivel de riesgo es elevado.
    b. Llevar a cabo una Evaluación de Impacto[93], debido a que se tratan con datos sensibles y al carácter innovador de las tecnologías empleadas. Esta consiste en analizar los riesgos del tratamiento de datos personales y así saber cuáles son las medidas de seguridad que se deben de implementar, cuyo ciclo genérico se señala en el Anexo 4.
7. Analizar la necesidad y proporcionalidad:

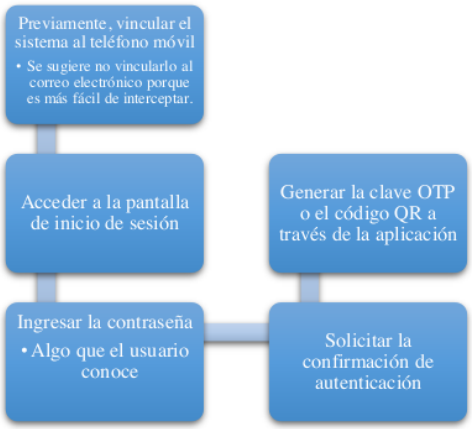
¿Se trata de una medida susceptible de conseguir el objetivo propuesto?	Sí, se asegura a nivel alto que quien ingresa a la plataforma es quien dice ser.
¿No existe otra medida más moderada para conseguir el objetivo con la misma eficacia?	Sí, usando OTP o código QR, para el caso de la autenticación. Otras medidas para evitar la compartición de cuentas se estudiarán en epígrafes posteriores.
¿Es una medida ponderada o equilibrada pues se obtienen más beneficios para el interés general que perjuicios sobre otros bienes en conflicto?	No. Es una medida intrusiva a la privacidad de los usuarios y la protección de sus datos personales. Los beneficios son menores que las pérdidas.

Del análisis anterior se desprende que el uso de datos biométricos como parte de la autenticación difícilmente puede considerarse como un método proporcionado y adecuado, pues solo cumple con uno de los tres requisitos. Por lo tanto, se aconseja que en caso de llevar a cabo el sistema 2FA, no se opte por el uso de los datos biométricos, ya que es una medida que podría considerarse excesiva para los fines, dado que se trata de datos personales sensibles. En su lugar, se pueden implementar otras opciones, como la OTP o mediante código QR, puesto que el nivel de impacto[94] del tratamiento mediante

[93] AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, (2019), Listas de tipos de tratamientos de datos que requieren evaluación de impacto relativa a protección de datos (art 35.4), pág. 2. Recuperado de: https://www.aepd.es/sites/default/files/2019-09/listas-dpia-es-35-4.pdf

[94] AGENCIA DE LA UNIÓN EUROPEA PARA LA SEGURIDAD CIBERNÉTICA (ENISA), (2016), Guidelines for SMEs on the security of personal data processing, pág. 20. Recuperado de: https://www.enisa.europa.eu/publications/guidelines-for-smes-on-the-security-of-personal-data-processing

el uso de datos biométricos es *alto*, mientras que si se emplea la OTP o el código QR puede reducirse a *medio* porque se tratan datos personales simples, por lo que se propone el siguiente proceso:



Asimismo, se sugiere que, este mecanismo se implemente únicamente cuando se detecte el inicio de sesión desde un dispositivo nuevo o desde otra dirección IP, puesto que implementarlo en cada inicio de sesión va a resultar molesto e incómodo para el usuario, orillándolo a buscar plataforma que sea más amable con el inicio de sesión.

5.3. Uso de sistemas biométricos

Como ya se mencionó en el epígrafe anterior, el uso de datos biométricos se ha vuelto muy popular en aras de identificar y autenticar a las personas, pues es la manera más efectiva para asegurarse que la persona es quien dice ser. No obstante, la seguridad se robustece cuando se usa el doble o multi factor de autenticación, mas no cuando se usa la biometría de manera aislada, ya que es un proceso de autenticación débil.

Como datos biométricos se puede utilizar el iris, la retina, la voz, las firmas, el reconocimiento facial o la huella dactilar, siendo este último el más utilizado, conocido también como *fingerprinting*, que consiste en "*una recopilación sistemática de información sobre un determinado dispositivo remoto con el objetivo de identificarlo, singularizarlo y, de esa forma, poder hacer un seguimiento de la actividad del usuario del mismo con el propósito de perfilarlo*".[95] El reconocimiento facial, por su parte, es una

[95] AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, (2019), Estudio Fingerprinting o Huella digital del dispositivo, pág. 4. Recuperado de: https://www.aepd.es/sites/default/files/2019-09/estudio-fingerprinting-huella-digital.pdf

técnica informática que se basa en la probabilidad con el objetivo de reconocer de forma automática a una persona para autenticarlo o identificarlo.[96] Aunque también hay quienes optan por la biometría multimodal y hacen combinaciones de estos indicadores biométricos.

La ventaja de utilizar la lectura de huella digital o el reconocimiento facial es que ambos son fáciles, rápidos y muy seguros. En caso de emplear este sistema, se le puede proporcionar a los clientes un dispositivo que utilice un marcador biométrico, como la huella dactilar, el cual podrá usarse para televisiones inteligentes. Para el caso de los teléfonos móviles, tabletas y ordenadores que no tengan incluida la función del uso de la huella dactilar, se puede hacer uso de la cámara y activar el reconocimiento facial. Para aquellos dispositivos que sí cuenten con la tecnología de lector de la huella dactilar, se puede habilitar la función para su teléfono o tableta y que sea el usuario que decida con qué dato biométrico quiere autenticarse, si por reconocimiento facial o a través de la huella.

La desventaja es que este sistema funciona muy bien con los dispositivos que tienen lector de huella integrado o una cámara, mas no con aquellos que no lo tienen, como las televisiones. Para esto, se necesitaría adquirir un dispositivo y tan solo la inversión en el hardware representa un costo alto, mismo que al final se le trasladaría al cliente, lo que incrementaría el precio de la suscripción y lo desalentaría a usar la plataforma de Netflix, orillándolo a que elija a la competencia.

Además, cabe destacar que el uso de sistemas biométricos por sí solo no es 100% preciso por los siguientes motivos: i) Se ha demostrado que los hermanos y familiares han llegado a esquivar y confundir un sistema biométrico de reconocimiento facial; ii) la huella dactilar puede ser burlada por réplicas o cortes; iii) las huellas dactilares se han visto afectadas con el envejecimiento de las personas; iv) las condiciones medio ambientales no contraladas, como la iluminación, también han influido en falsos positivos o en que una persona no pueda acceder, aun tratándose de ser quien dice ser; y v) no todas las personas son aptas para este sistema, tales como aquellas que presenten lesiones o

[96] COMISIÓN NACIONAL DE INFORMÁTICA Y DE LAS LIBERTADES (CNIL), (2019), Reconnaissance Faciale. Pour un Debat à la Hauteur des Enjeux, pág. 3. Recuperado de: https://www.cnil.fr/sites/default/files/atoms/files/reconnaissance_faciale.pdf

problemas de salud.[97] También hay que tomar en cuenta que en muchas ocasiones los usuarios sienten que su privacidad se invade al usar algún dato biométrico.

5.3.1. Implicaciones jurídicas

Jurídicamente, un dato biométrico se refiere a los "*datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos*"[98]. En caso de optar por el uso de un dato biométrico, se sugiere que este sea la huella dactilar, por ser el más cómodo para el usuario.

Además, es importante tomar en cuenta que, como ya se mencionó en epígrafes anteriores, un dato biométrico es un dato sensible, se deben de tomar las medidas señaladas en el Anexo 3.

En caso de no llevarse a cabo de esta manera, se considera una infracción muy grave, consistente en una multa de hasta 20 millones de euros o de una cuantía máxima que equivalga al 4% del volumen del negocio total anual global, lo que resulte más alto.[99] Además de una indemnización a los usuarios por los daños y perjuicios materiales e inmateriales causados[100]

Además, se le debe de ofrecer otra alternativa para ingresar al sistema de Netflix, de manera que el medio biométrico no sea la única forma para acceder. Puede emplearse en caso de que salte alguna alarma en caso de que un tercero no autorizado acceda a la cuenta, mas no como medio ordinario de acceso al servicio, ya que entonces no se estaría otorgando el consentimiento libremente, pues el usuario no estaría siendo libre de elegir y quedaría invalidado[101], por lo que no es admisible que, como consecuencia de denegar el consentimiento, se les negara a los usuarios la posibilidad de acceder a la plataforma de Netflix.

---

[97] AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, *Loc. Cit.*
[98] Artículo 4.14 del RGPD.
[99] Artículo 83.5.a del RGPD.
[100] Artículo 82 del RGPD.
[101] GRUPO DE TRABAJO DEL ARTÍCULO 29, (2018), Directrices sobre el consentimiento en el sentido del Reglamento (UE) 2016/679, pág. 6. Recuperado de https://www.avpd.euskadi.eus/contenidos/informacion/20161118/es_def/adjuntos/wp259rev01_es20180709.pdf

Por otra parte, así como en el epígrafe anterior es necesario realizar un análisis de proporcionalidad y determinar si la implementación de sistemas biométricos por sí solos cumple con los siguientes requisitos:

¿Se trata de una medida susceptible de conseguir el objetivo propuesto?	Sí, se asegura a nivel bajo que quien ingresa a la plataforma es quien dice ser.
¿No existe otra medida más moderada para conseguir el objetivo con la misma eficacia?	Sí, se estudiarán en epígrafes posteriores.
¿Es una medida ponderada o equilibrada pues se obtienen más beneficios para el interés general que perjuicios sobre otros bienes en conflicto?	No. Es una medida intrusiva a la privacidad de los usuarios y la protección de sus datos personales. Los beneficios son menores que las pérdidas.

Del análisis anterior se desprende que el solo uso de sistemas biométricos difícilmente puede considerarse proporcionado y adecuado, pues solo cumple con uno de los tres requisitos, además, de que se pueden valorar otros métodos menos intrusivos para la privacidad de los usuarios, como se analizará más adelante.

5.4. Asociación a dispositivos específicos

Esta medida consiste en limitar el número de dispositivos en donde se encuentre activa la plataforma. Al llegar al límite de dispositivos permitidos, si no se elimina un dispositivo de la lista, no se pueden agregar otros nuevos. La posible solución sería que Netflix limitara el número de dispositivos que se pueden tener en una cuenta, como lo siguiente:

Plan	Pantallas que se pueden ver al mismo tiempo	Máximo de dispositivos permitidos
Básico	1	2
Estándar	2	4
Premium	4	8

Se sugiere que, en el plan básico, pensando en que sea para una sola persona, sean dos dispositivos máximos, el de la televisión principal u ordenador y el de una tableta o móvil, por ejemplo, que es lo más usual. El plan estándar, tomando en cuenta que son dos pantallas las que se pueden ver al mismo tiempo y pensando que tal vez es para una pareja, sean amigos, novios o esposos, o el caso del hijo que se va a la universidad y que sigue dependiendo de la cuenta pagada por sus padres o tutores, se piensa que tal vez cada uno puede tener dos dispositivos donde ver Netflix. El plan premium, que está pensado para

una familia de al menos 4 personas, igualmente se piensa que cada uno tenga dos dispositivos en los que pueda vincular la cuenta. Probablemente se considere que son muchos dispositivos vinculados, pero se sugiere que sean ocho como máximo y cuatro como mínimo, tomando en cuenta que cada persona cuenta con al menos dos dispositivos.

Cuando los usuarios inicien sesión por primera vez en un dispositivo se sugiere que aparezca el siguiente mensaje:

> Este es el primer dispositivo que vinculas a tu cuenta Netflix. Tú cuentas con el plan [*indicar plan*] por lo que tienes derecho a vincular [*números de dispositivos*] más. Después de esto, podrás vincular dispositivos hasta alcanzar el límite de [*número máximo de dispositivos conforme al plan contratado*].

Cuando los usuarios inicien sesión en un último dispositivo al que tienen permitido, se sugiere que aparezca el siguiente mensaje:

> Al vincular este dispositivo ya no tendrás permitido vincular más dispositivos. En caso de necesitar vincular otro, deberás desvincular uno de los que ya tengas dados de alta en la sección de **Cuenta**.

En caso de que el usuario quiera iniciar sesión en otro dispositivo que no está dado de alta, se sugiere que aparezca el siguiente mensaje:

> Has excedido el número de dispositivos vinculados permitidos. Si necesitas vincular este dispositivo tienes que desvincular algún otro que ya no utilices en la sección de **Cuenta.**

Si bien Netflix tiene un límite con respecto a las pantallas a visualizar al mismo tiempo, no tiene un límite acerca del número de dispositivos que pueden estar vinculados a la cuenta. Si se implementa este sistema va a resultar tedioso para los usuarios compartir las contraseñas y estar eliminando y dando de alta dispositivos frecuentemente, pues hay usuarios titulares de cuentas que tienen iniciada sesión en el móvil, en la tableta, el computador y la televisión.

5.4.1. Implicaciones jurídicas

A diferencia de las anteriores sugerencias, esta medida no tiene ninguna implicación en cuanto a datos personales de manera directa. No obstante, se sugiere que en los términos de uso se agregue una cláusula que contenga la información descrita anteriormente. Por lo que se sugiere la siguiente redacción de la Cláusula 4.3:

> 4.3. Puedes ver el contenido de Netflix principalmente dentro del país en el que hayas establecido tu cuenta y solo en las ubicaciones geográficas donde ofrezcamos nuestro servicio y hayamos licenciado dichos contenidos. El contenido disponible para visionado varía en función de la ubicación geográfica y cambia periódicamente. Además, podrás ver el contenido en los dispositivos que tengas vinculados a tu cuenta. El número de dispositivos en los que puedes ver contenidos de forma simultánea, así como la cantidad de dispositivos que puedes vincular a tu cuenta, dependen de tu plan de suscripción y está especificado en la página "Cuenta".

Lo que se debe de hacer es aplicar las medidas técnicas y organizativas óptimas para proteger el acceso al sistema a personas no autorizadas, tomando en cuenta el estado del desarrollo tecnológico, los costos de implementación, el propósito del procesamiento y la revisión periódica. En todo caso, se debe garantizar la confidencialidad, la integridad, la disponibilidad y la resiliencia, la capacidad de restaurar la disponibilidad de los datos y su acceso. De no hacerlo, el incumplimiento a estas obligaciones conlleva al pago de una multa de hasta 20 millones de euros o hasta el equivalente al 4% del volumen del negocio total anual global, lo que resulte mayor[102] más el pago de daños y perjuicios a los usuarios afectados.

5.5. Uso de geolocalización

La geolocalización emplea los datos de los dispositivos conectados a Internet con el propósito de identificar en un mapa la ubicación física de una persona. Actualmente, es muy utilizada por varias aplicaciones, pues les ayuda a las empresas a alcanzar sus objetivos, que pueden ser ubicar propiamente a sus usuarios o personalizar el contenido que se le proporciona. La geolocalización se puede recopilar de dos formas:

a) Activo. Mediante el uso del firmware y el software del dispositivo del usuario, empleando el GPS, WiFi y las redes 3G, 4G y 5G.

[102] Artículo 83.5.a del RGPD.

b) Pasivo. Mediante el uso de los datos contenidos en los servidores, utilizando la dirección IP.

Actualmente, Netflix utiliza la geolocalización porque con base en la región en la que el usuario se encuentre, es el tipo de contenido que le va a ofrecer, de conformidad con las licencias que tenga Netflix en dicho lugar. No obstante, no utiliza la geolocalización como lo hace Spotify, por ejemplo, para monitorear que los usuarios que comparten cuentas realmente vivan en el mismo domicilio, como es la forma en la que Netflix permite que esto ocurra.

Al emplearla, Netflix monitorearía de vez en vez la geolocalización de los usuarios para saber desde dónde está visualizando el servicio y verificar que efectivamente lo realiza desde su domicilio. La desventaja sería en el caso de las segundas residencias, cuando las personas se vayan de vacaciones, se encuentren de visita en la casa de alguna otra persona, lo utilicen en la escuela o incluso en el transporte público ya que, en muchas ocasiones, aunque no se comparta la cuenta, es la misma persona dada de alta la que lo utiliza, pero en diferentes ubicaciones. De manera que podría dar lugar erróneamente a detectar un supuesto mal uso de la cuenta y se le suspendería o cancelaría a alguien que sí la está usando legítimamente, lo que causaría inconformidades y molestias al usuario.

5.5.1. Implicaciones jurídicas

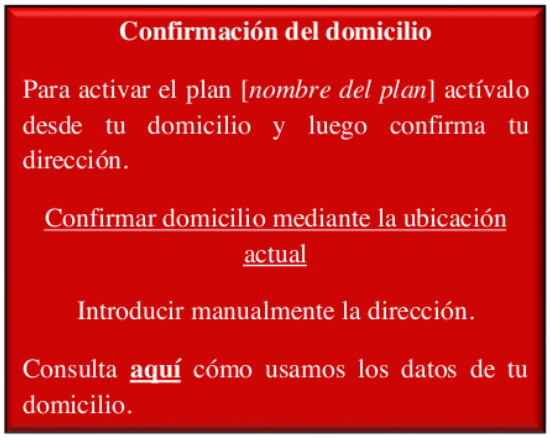
La geolocalización es una injerencia a la vida privada de las personas pues no solo permite individualizar al usuario, sino que también permite incluso conocer cuáles son los hábitos de las personas. Además, con los dispositivos, la posibilidad para identificar a una persona es directa e indirecta[103], ya que a través del operador de telecomunicaciones se tiene acceso a datos personales como nombre y dirección de cada cliente, los números únicos de su dispositivo (dirección MAC), así como el IIEM/IMSI. Por otra parte, a través de las aplicaciones se obtienen datos de identificación directos. Por lo tanto, al no anonimizarse y vincular directamente a una persona, se trata de datos personales[104], de manera que le es aplicable el Reglamento General de Protección de Datos (en adelante "RGPD").

[103] GRUPO DE TRABAJO SOBRE PROTECCIÓN DE DATOS ESTABLECIDO POR EL ARTÍCULO 29, (2011), Dictamen 13/2011 sobre los servicios de geolocalización en los dispositivos móviles inteligentes, pág. 10. Recuperado de: https://www.apda.ad/sites/default/files/2018-10/wp185_es.pdf

[104] Artículo 4.1 del RGPD.

Por lo anterior, las obligaciones a las que quedaría sujeto Netflix en caso de adoptar esta medida son las siguientes:

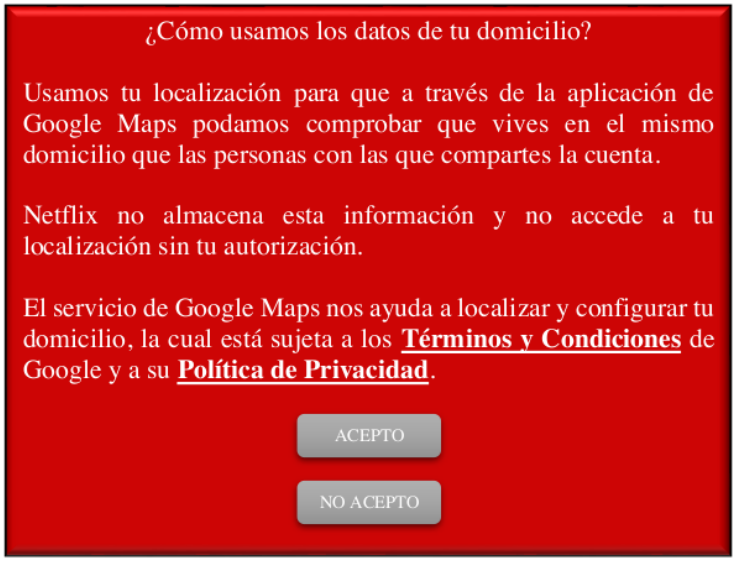
1. En primer lugar, se sugiere que únicamente sea válida en los planes Estándar y Premium, ya que en caso de que el usuario se niegue a activar la geolocalización, se le dé la opción de adquirir el plan básico, de manera que el usuario no se vea obligado a consentir otorgar la geolocalización y tenga otra opción que no sea tan intrusiva con sus datos. Es un esquema bastante semejante al de Spotify pero que ha dado resultados.
2. Netflix es responsable del tratamiento de los datos personales.
3. El procesamiento de los datos de geolocalización debe de ajustarse a lo establecido en el RGPD, debe de ser justo, transparente y limitarse al propósito establecido, que es el de verificar que se cumple con los requisitos establecidos para hacer uso de los planes y se debe de asegurar a los usuarios la seguridad de dichos datos[105].
4. Adoptar las medidas técnicas y organizativas adecuadas, mismas que deben actualizarse frecuentemente.
5. La base de legitimación es el cumplimiento de un contrato. No obstante, se recomienda solicitar el consentimiento previo[106] a que la aplicación recoja los datos, por lo que se sugiere que, al momento de crear la cuenta, aparezca el siguiente mensaje:



[105] Artículo 5.1 del RGPD.

[106] AUTORIDAD HOLANDESA DE PROTECCIÓN DE DATOS, (2011), Report of findings. Official investigation by the CBP into the processing of geolocation data by TomTom N.V. Recuperado de: https://autoriteitpersoonsgegevens.nl/sites/default/files/downloads/mijn_privacy/en_pb_20120112_investigation-tomtom.pdf

Al momento de que el usuario dé clic a "aquí", se sugiere que aparezca la primera capa, cuyo texto recomendado es el siguiente:



En esta capa se le informará al usuario que puede consultar más información al respecto accediendo a la segunda capa, que es la Política de Privacidad.

6. Deber de información y de transparencia. En la política de privacidad se debe especificar claramente el dato recabado y el uso que se le dará a la información obtenida, de forma clara y sencilla[107]. Por lo tanto, esta debe de agregarse. Se sugiere el siguiente texto:

Uso de información

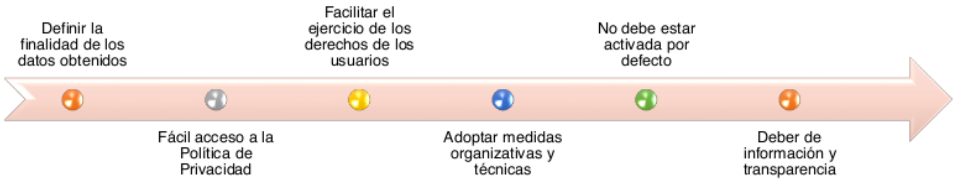
[…]

- Verificación de plan para los usuarios con los planes Estándar y Premium. Mediante la ayuda de la aplicación de Google Maps localizamos su dirección con el único objeto de verificar que se cumplen los requisitos de los planes. Estos datos se usarán únicamente durante el tiempo que esté suscrito al servicio.

La información de la Política de Privacidad debe ser fácilmente accesible desde cualquier dispositivo que se visualice Netflix, como hasta ahora.

[107] Artículo 25 del RGPD.

7. Privacidad por diseño y por defecto. La geolocalización no debería de estar habilitada por defecto para usarla en todo momento, sino que se le debe de dar la opción al usuario de que esta se utilice únicamente mientras se utiliza la aplicación de Netflix, de manera que se permita deshabilitar la geolocalización cuando su uso no sea estrictamente necesario, pues el objetivo de Netflix es verificar que vive en el domicilio mientras disfruta del servicio, no mientras hace alguna otra actividad.
8. Evaluación de Impacto. Si bien no se elaborarán perfiles, sí es importante realizarla puesto que existe un tratamiento a gran escala de datos personales, como lo es la geolocalización. Esta se debe de realizar tomando en cuenta el punto 8.1 del Anexo 3 y el Anexo 4.
9. Nombrar un Delegado de Protección de Datos, toda vez que se emplean datos a gran escala, además de que la geolocalización es un dato personal.[108]
10. Facilitarles a los usuarios el ejercicio de sus derechos.
11. Se sugiere no guardar las localizaciones que se obtengan.



En caso de incumplir con estas recomendaciones, Netflix puede ser acreedor a una multa que puede ser hasta de 20 millones de euros o la cantidad equivalente al 4% de la facturación anual total mundial, lo que resulte mayor,[109] además de una indemnización a los usuarios por los daños y perjuicios materiales e inmateriales causados por no tener una buena medida de seguridad[110]. La otra consecuencia sería la mala reputación hacia Netflix, pues cumplir con las normas de protección de datos proporciona seguridad a los usuarios y a los posibles futuros usuarios.

5.6. Bloqueo basado en la IP

Mediante la IP (Protocolo de Internet) es posible localizar e identificar un dispositivo, puesto que esta dirección es única, se utiliza para transportar información en internet y

[108] Artículo 37.1 del RGPD y previsto así por el Grupo de Trabajo del artículo 29.
[109] Artículo 83.3 del RGPD.
[110] Artículo 82 del RGPD.

define la manera en la que la información se envía entre servidores y dispositivos. En este caso, la idea consiste en bloquear el acceso a Netflix de una dirección IP de la que se sospeche que se está haciendo un mal uso de la cuenta de Netflix. No obstante, estas direcciones IP son privadas, es decir, *"se utilizan para identificar un dispositivo dentro de la red privada"*[111], como la que se obtiene de un teléfono inteligente, una televisión inteligente, el ordenador o una tableta.

5.6.1. Inconvenientes

Esto no es tan preciso, pues los usuarios pueden hacer uso de una VPN (Virtual Private Network o Red Privada Virtual) para navegar de forma anónima o incluso mostrar una dirección IP diferente a la real, que se puede ubicar en cualquier parte del mundo, esto con el objeto de que ya no se pueda rastrear el dispositivo desde el que se conecta el usuario. De esta forma, eluden las medidas de restricción de contenido por parte de Netflix, evitando el bloqueo geográfico.

En este sentido cabe hacer mención también que si bien existe el Reglamento UE 2017/1128, en el que se obliga a los prestadores de servicio audiovisual en línea de pago a mostrar el mismo catálogo sin importar en qué parte de la Unión Europea se encuentren los clientes, debido a la portabilidad fronteriza de contenidos en línea, esto no es del todo posible de llevar a la práctica, puesto que obedece a restricción en materia de propiedad intelectual, debido a las licencias que obtiene Netflix las cuales, en algunas ocasiones, limitan la reproducción de las obras audiovisuales a determinados países. De manera que la portabilidad fronteriza solo es posible en los lugares en los que Netflix tenga los derechos de las obras audiovisuales, sin importar que sea dentro de la misma Unión Europea. Es por esta razón que muchos usuarios utilizan VPNs para poder acceder a contenido de Netflix que está disponible en otras regiones. Al respecto, Netflix ya ha tomado cartas en el asunto desde 2016 y utiliza bloqueadores.

5.6.2. Implicaciones jurídicas

Las direcciones IP son datos de una persona identificable[112], por lo que sí constituyen datos personales[113], especialmente en los casos en los que el objeto consiste en identificar

---

[111] BARRIOS ANDRÉS M., (2020), *Manual de Derecho Digital*, Tirant Lo Blanch, pág. 46.

[112] Aquella persona cuya identidad se puede identificar directa o indirectamente, de conformidad con el artículo 4 del RGPD.

[113] SAN 01 de septiembre de 2011, Rec. 625/2009; STS, Tercera Sala, 03 de octubre de 2014, en España; por el TJUE en el asunto C-70/10 Scarlet Extended (Grupo Belgacom) vs Sabam Sase de 2011. También

a los usuarios de un dispositivo, aunque se trate de direcciones IP dinámicas,[114] siempre y cuando se cumpla con dos condiciones:[115]

a) El ISP puede vincular la dirección IP dinámica a la identidad de un usuario.
b) La aplicación cuenta con un medio legal para tener acceso a la información en manos del ISP.

Además, el tratamiento de la IP como dato personal se considerará lícito si es necesario para satisfacer el interés legítimo del responsable del tratamiento. De tal manera que, si la aplicación cuenta con los medios legales para obligar al ISP a revelar la información necesaria para identificar a los usuarios y satisface el interés legítimo, entonces la dirección IP de los usuarios será considerada un dato personal que estaría en manos de la aplicación.

En el caso particular, esto se cumpliría porque el proveedor de servicios de Internet con el que Netflix realice la negociación tiene registrada la dirección IP dinámica que se le designa a un dispositivo determinado en cierto momento y sabe a quién se le asigna. Por su parte, Netflix cuenta con el registro de las direcciones IP dinámicas de quienes acceden a la plataforma. Al combinar la información de ambos, Netflix puede identificar quién está detrás de las direcciones dinámicas IP que acceden a su plataforma y corroborar si se trata de usuarios registrados o no. De manera que, al contar Netflix con la información suficiente para vincular la dirección IP a un cliente en particular, ya sea a través de las cookies o del inicio de sesión, la dirección IP es un dato personal y debe entonces darle el tratamiento adecuado como tal conforme a lo establecido en el RGPD. Pero para esto, hay que analizar primeramente si el ISP puede proporcionarle esa información a Netflix o no.

¿El ISP puede proporcionarle a Netflix la información de sus clientes? Es decir, ¿hacer la combinación de datos conforme a lo descrito en párrafos anteriores es razonable? Es un

---

es reconocido como dato personal por la Comisión Europea en https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_es; recogido así en el Considerando 30 del RGPD y criterio que sigue la AEPD conforme al informe 327/2003.

[114] GRUPO DE TRABAJO DEL ARTÍCULO 29, (2007), Dictamen 4/2007 sobre el concepto de datos personales, pág. 18. Recuperado de: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_es.pdf.

[115] Tribunal de Justicia de la Unión Europea, 19 de octubre de 2016, asunto 582/14 Patrick Breyer vs Alemania.

medio razonable siempre y cuando la identificación del cliente no esté prohibida por ley o sea casi irrealizable en cuestión de costes, tiempo y recursos humanos[116].

En ese sentido, las legislaciones de los países de la Unión Europea son unánimes al considerar que, de principio, los ISP no tienen permitido transmitirle directamente a un tercero información sobre sus clientes, excepto si estos terceros recurren a la vía penal ante la autoridad competente alegando la comisión de algún delito informático, como los ataques cibernéticos, por ejemplo.

En el caso específico de España, los operadores están obligados a conservar los datos que se generen o que se traten con motivo del servicio prestado, dentro de los cuales se encuentran: el nombre, dirección del abonado o usuario registrado al que se le ha asignado una dirección IP[117], y a ceder dichos datos únicamente con autorización judicial con fines de detección, investigación y enjuiciamiento de delitos graves tipificados en el Código Penal o leyes especiales.[118]

De conformidad con lo anterior, no es posible llevar a cabo esta medida más que previa denuncia, pero se recuerda que en Europa la compartición de cuentas no constituye un delito, en todo caso, procedería a solicitar la información tratándose de crímenes como fraudes o piratería, pero dicha problemática no es objeto de estudio del presente informe.

Ahora bien, descartando esa opción se procede a analizar si fuese posible justificar la cesión de información alegando que satisfaría el interés legítimo de Netflix, y demostrando que esta restricción se establecería sin sobrepasar los límites de lo estrictamente necesario. Cabe destacar aquí que de todas las bases legitimadoras para el tratamiento de datos personales el interés legítimo es la más compleja de todas.

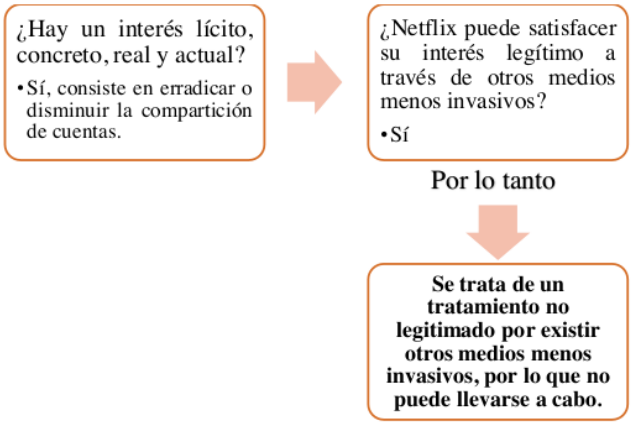
No se puede invocar el interés legítimo sin hacer una ponderación entre dicho interés de Netflix (quien va a tratar los datos) y los derechos fundamentales de los interesados y determinar cuál prevalece, de manera que se procede a realizar dicha ponderación:

---

[116] *Ibidem*.

[117] Artículo 3.2.iii) de la Ley 25/2007 de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones.

[118] Artículo 6 de la Ley 25/2007 de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones.



Derivado de lo anterior, al estar prohibido por una ley y al no ser el interés jurídico una base jurídica suficiente, es que este método no podría llevarse a cabo en la Unión Europea. De llevarse a cabo, el tratamiento sería ilegítimo y daría lugar a una multa para Netflix que puede ser hasta de 20 millones de euros o la cantidad equivalente al 4% de la facturación anual total mundial, lo que resulte mayor, además de una indemnización a los usuarios por los daños y perjuicios materiales e inmateriales causados[119]

5.7. Uso de inteligencia artificial, aprendizaje automático y análisis de comportamiento

El objetivo de estas tecnologías es desarrollar un perfilado de los clientes, es decir, se va a inferir mayor información sobre ellos mediante la evaluación, análisis y/o predicción de aspectos personales.[120] Para ello, la empresa Synamedia[121], cuenta con un software que fue presentado en el CES 2019, mediante el uso de la tecnología que ellos llaman *Credentials sharing insight*, que funciona como un producto independiente que se integra a la aplicación y que emplea la inteligencia artificial, el aprendizaje automatizado y el análisis de comportamiento para identificar, analizar y rastrear las credenciales de las cuentas de los suscriptores. Es decir, hace un análisis predictivo para detectar el intercambio de contraseñas, además, analiza los casos de robos de identidad.

Lo anterior se resume en la creación de algoritmos de aprendizaje automático, análisis de comportamiento de los usuarios y la inteligencia humana[122] que, de conformidad con el

[119] Artículo 82 del RGPD.
[120] Artículo 4.4 del RGPD.
[121] Compañía de Reino Unido encargada de proveer soluciones de video.
[122] El sitio de synamedia lo denomina “inteligencia colectiva”.

portal de Synamedia,[123] estos algoritmos van a permitir detectar con precisión las anomalías en el comportamiento de los usuarios, como lo es la compartición de cuentas, al estar monitoreando el dispositivo, cuándo, dónde se usa y por cuánto tiempo se usa. Es decir, con este programa se construyen patrones de comportamiento.

De esta forma, saltarán las alarmas si se llega a detectar que una misma cuenta está sincronizada al mismo tiempo en dos lugares diferentes. No obstante, esto no puede ser motivo de que se cancele inmediatamente la cuenta del usuario, ya hay que tomar en cuenta también otros factores porque puede que, por ejemplo, el usuario se encuentre de viaje. Pero Synamedia asegura que su algoritmo es tan efectivo que permite detectar sin problemas esta situación, así como la detección de si un usuario tiene hijos que viven fuera del núcleo familiar, de manera que Netflix no castigue de forma errónea la compartición de cuentas que sí están legitimadas, pues los puntos que hay que tomar como referencia son los hábitos de visualización de la población y el conocimiento de las regulaciones locales. A la par, se puede también generar una base de datos con las cuentas y las contraseñas detectadas como fraudulentas y determinar los patrones que se siguen.

Una vez que se ha generado el algoritmo, Netflix puede hacer tres cosas: i) activar medidas de seguridad; ii) desarrollar marketing personalizado; o iii) ambas. El punto es comprobar si las cuentas que saltan las alarmas como "posibles cuentas fraudulentas" en realidad lo son o solo se tratan de posibles clientes, sin vulnerar el servicio del verdadero suscriptor.

En el primer caso, el mecanismo a emplear puede consistir en solicitarle al usuario que restablezca su contraseña, forzándolo a que cierre la sesión en todos los dispositivos que tenga conectados. De esta manera, Netflix podrá frenar el uso de las cuentas fraudulentas, pues solo se quedarían activados los dispositivos reales del usuario.

En el segundo caso, y toda vez que Netflix no cuenta con anuncios publicitarios dentro de su contenido, el marketing le podría llegar al usuario a través de correo electrónico o

[123] https://www.synamedia.com/video-solutions/video-security/credentials-sharing/

mediante un anuncio que aparezca en forma de banner que puede ser cerrado manualmente por el usuario. Se sugiere el siguiente diseño y texto:

O bien, pueden llevarse a cabo ambas acciones a la par.

La ventaja es que no solo ayudaría a mitigar la compartición de cuentas, sino que también es una medida contra la piratería, cuyo tema no es objeto de estudio en el presente documento. Al momento de que se le priva el servicio a una persona una vez que ya ha disfrutado del contenido, esta persona puede convertirse en un posible usuario.

5.7.1. Implicaciones jurídicas

Toda vez que se va a monitorizar el comportamiento de los usuarios, usar inteligencia artificial basado en el análisis de información personal de miles de usuarios, es decir, empleando el *big data*, es necesario cumplir con lo establecido en el RGPD, máxime que se va a realizar perfilado y de los clientes conforme a lo establecido en el artículo 4.4 del RGPD y se tomarán decisiones automatizadas, puesto que se llevarán a cabo de la siguiente forma[124]:

- Es una forma automatizada del tratamiento.
- Se lleva a cabo respecto de datos personales de los clientes.
- El objeto evalúa aspectos personales de personas físicas, es decir, los clientes.

Para ello, hay que garantizar los derechos y las libertades, cumpliendo con las siguientes obligaciones, que se explican a mayor detalle en el Anexo 5:

1. El sistema de Synamedia debe de respetar la dignidad humana, la libertad, los derechos humanos de los usuarios, estar adecuado a la normativa europea y respetar los principios éticos.[125]

[124] GRUPO DE TRABAJO SOBRE PROTECCIÓN DE DATOS DEL ARTÍCULO 29, (2018), Directrices sobre decisiones individuales automatizadas y elaboración de perfiles a los efectos del Reglamento 2016/679, pág. 7. Recuperado de: https://www.aepd.es/sites/default/files/2019-12/wp251rev01-es.pdf

[125] COMISIÓN EUROPEA, (2019), Generar confianza en la inteligencia artificial centrada en el ser humano, COM (2019) 168 final, pág. 3. Recuperado de: https://ec.europa.eu/transparency/regdoc/rep/1/2019/ES/COM-2019-168-F1-ES-MAIN-PART-1.PDF

2. Es importante asegurarse que el sistema de Synamedia cumple con los siete requisitos esenciales establecidos por la Comisión Europea:[126]
   a. Sea intervenido y supervisado por los humanos.
   b. Tenga solidez y seguridad técnicas.
   c. Prime la privacidad y gestión de datos recabados en todas las fases.
   d. Transparencia.
   e. Cumpla con la diversidad, no discriminación y equidad.
   f. Cumpla con el bienestar social.
   g. Rinda cuentas a Netflix.
3. Evaluar las soluciones del sistema, conforme a parámetros que deben de especificarse[127].
4. Determinar quién es el responsable y quién es el encargado en las etapas del ciclo de vida del sistema.

El sistema de Synamedia debe cumplir con los siguientes requisitos que deben evaluarse en todo el ciclo de vida del sistema:

- Intervención y supervisión humanas
- Solidez y seguridad técnicas
- Privacidad y gestión de datos
- Transparencia
- Bienestar, no discriminación y equidad
- Bienestar social
- Rendición de cuentas

El responsable del tratamiento debe de atender lo siguiente:

5. Legitimación y limitación del tratamiento. La base de legitimación sería contractual.[128]
6. Deber de información. Netflix debe informar el tratamiento de los datos de forma clara, visible, accesible, sencilla y transparente, con el objeto de que los usuarios sean conscientes de la interacción que tienen con el sistema y entiendan los resultados.
7. Transparencia[129]. Este es un aspecto crítico para este sistema, por lo que es importante nombrar un Delegado de Protección de Datos[130].
8. Limitación de la finalidad. Los datos se deben usar solo para el fin específico, que es detectar la compartición de cuentas en supuestos no autorizados por Netflix.
9. Minimización de los datos. Para poder llevar a cabo el tratamiento es necesario usar solamente los datos mínimos que se requieran para ello, no más, es decir, que son los

[126] *Ibid,* pág. 4.
[127] AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, (2020), Adecuación al RGPD de tratamientos que incorporan Inteligencia Artificial. Una introducción, pág. 15. Recuperado de: https://www.aepd.es/sites/default/files/2020-02/adecuacion-rgpd-ia.pdf
[128] Artículo 22.2 del RGPD.
[129] Considerando 78 en relación con los artículos 39 y 58 del RGPD.
[130] Conforme al artículo 37.1 del RGPD es obligatorio por tratar datos a gran escala.

adecuados, los pertinentes y los limitados. Por eso es importante conocer cuáles son los datos que recaba el sistema, de conformidad con Synamedia.

10. Precisión estadística. Se deben usar los procedimientos matemáticos o estadísticos que sean adecuados para el tratamiento, que garanticen la fidelidad e integridad de que los datos de los usuarios son exactos, por lo que es importante documentar todo.
11. Limitación del plazo de conservación. Los datos se deben conservar únicamente por el tiempo estrictamente necesario, es decir, durante el tiempo en el que el se tenga la calidad de usuario por utilizar el servicio de Netflix.
12. Integridad y confidencialidad. Los datos deben tratarse de tal manera que se garantice la seguridad adecuada de los datos de los usuarios, mediante la aplicación de las medidas técnicas y organizativas más apropiadas.
13. Responsabilidad proactiva. Debe de incorporar garantías más allá de las mínimas para gestionar los riesgos que lleguen a presentarse.
    - Realizar un Análisis de riesgos.
    - Realizar una Evaluación de Impacto[131], toda vez que se evaluarán de forma sistemática y exhaustiva datos personales de los usuarios y se elaborarán perfiles. Además, los datos personales se tratarán a gran escala. Debe contener lo establecido en el punto 8.1 del Anexo 3, y el ciclo genérico para hacerlo se señala en el Anexo 4. Esta es una herramienta preventiva para considerar por qué y cómo se utiliza el sistema, que permite procesar los datos personales, analizar, evaluar y tratar los riesgos de las actividades.[132]
    - Contar con un método para gestionar los riesgos en el que se apliquen atenuantes y eximentes[133].
    - Estándar ISO 31000 sobre gestión de riesgos.
14. Evaluación de proporcionalidad. Establecer el impacto que tiene en el uso del sistema, mediante el análisis de proporcionalidad y necesidad[134]:

---

[131] AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, (2019), Listas de tipos de tratamientos de datos que requieren evaluación de impacto relativa a protección de datos (art 35.4), pág. 2. Recuperado de: https://www.aepd.es/sites/default/files/2019-09/listas-dpia-es-35-4.pdf

[132] BONMATÍ SÁNCHEZ J. y GONZALO DOMÉNECH J.J., (2020), La gestión de riesgos y su encaje legal en la regulación de la inteligencia artificial, En Arrabal Platero P., Doig Díaz Y., et. al. (Coord.), *Era digital, sociedad y derecho,* Tirant Lo Blanch, pág. 123.

[133] Se puede seguir el método establecido en el artículo 31.5 del Código Penal

[134] Artículo 35.7.b del RGPD.

¿Se trata de una medida susceptible de conseguir el objetivo propuesto?	Sí, se asegura a nivel alto que quien ingresa a la plataforma es quien dice ser.
¿No existe otra medida más moderada para conseguir el objetivo con la misma eficacia?	Existen otras medidas, pero aparentemente esta medida es la que garantiza una mayor eficacia.
¿Es una medida ponderada o equilibrada pues se obtienen más beneficios para el interés general que perjuicios sobre otros bienes en conflicto?	Si se cumplen con las recomendaciones, sí es una medida ponderada y equilibrada,

15. Seguridad de los datos.

Se deben de observar todas las medidas de seguridad, pues de lo contrario, daría lugar a una multa para Netflix que puede ser hasta de 20 millones de euros o la cantidad equivalente al 4% de la facturación anual total mundial, lo que resulte mayor. Además de una indemnización a los usuarios por los daños y perjuicios materiales e inmateriales causados[135].

16. Auditoría.
17. Transferencias internacionales. Los flujos transfronterizos a terceros países fuera del Espacio Común Europeo deben de contar con las garantías para que las transferencias se realicen con fluidez.

5.8. Concientizar acerca de los peligros de la compartición de contraseñas

El problema de la compartición de contraseñas no solo perjudica a Netflix, sino también a los mismos usuarios, pues al hacerlo, la seguridad de sus datos queda comprometida, y estos se exponen a la reventa de cuentas, ya sea tanto en la web convencional como en la *deep web*, o a que los "*hackers*" reactiven las cuentas que ya se habían cancelado. Incluso, debido al robo de contraseñas, mismas que fueron puestas a la venta en la *dark web*, varios usuarios dejaron de tener acceso a sus cuentas.

De conformidad con el ya citado estudio hecho en octubre de 2019, por Harris Poll en asociación con Google, el 43% de los estadounidenses ha compartido su contraseña con alguien más, y el 22% la ha compartido para algún servicio de televisión o video vía *streaming*. Pero esto no es lo más grave, sino que muchas personas utilizan la misma

[135] Artículo 82 del RGPD.

contraseña para sus demás cuentas; en concreto, el 66% de los estadounidenses, de conformidad con este mismo estudio.

Al respecto, el INCIBE y la AEPD[136] han señalado que esto implica un riesgo de seguridad, la información y los datos de las personas quedarían expuestos, pues no solo se tendría acceso a una cuenta de usuario, sino también porque los demás pueden curiosear con la información que obtienen, en el menor de los casos, porque en el peor de los casos, esto puede dar lugar a que actividades fraudulentas se lleven a cabo a nombre de las personas.

Por otra parte, el ya citado estudio reveló que el 40% de los encuestados dijo que su información personal ha sido comprometida; el 47% de esa información se tradujo en pérdidas de dinero, y el 12% dijo haber perdido más de 500 dólares. Aun así, solo el 45% de los estadounidenses cambia su contraseña incluso después de haber sido comprometida o de haber sufrido una violación de datos.

En noviembre de 2019, miles de cuentas de usuarios de Disney+ fueron hackeadas y sus contraseñas fueron puestas a la venta en la *dark web*[137]. Los usuarios de Netflix ya han sufrido de estos ataques, pues de conformidad con la BBC[138], varios usuarios publicaron en Twitter que les habían hecho cargos, siendo que ya habían cancelado su suscripción con antelación. Esto ocurre porque Netflix guarda la información de sus clientes por 10 meses, en caso de que se arrepientan y decidan regresar a la plataforma. Los "*hackers*" se aprovechan de esto y a través de *malwares*[139], *phishing* o de la simples compartición de cuentas, acceden a los datos de correo y de contraseña y se apropian de ellos.

Al respecto, no se le puede culpar a Netflix, pues cuenta con dos opciones seguras para los usuarios. La primera de ellas consiste en que los usuarios pueden mandar un correo electrónico a Netflix solicitando que eliminen sus datos de forma inmediata, sin tener que esperar los 10 meses. La segunda medida consiste en que cuando las cuentas se reactivan,

---

[136] AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS e INSTITUTO NACIONAL DE CIBERSEGURIDAD, Privacidad y Seguridad en Internet, pág. 6. Recuperado de: https://www.aepd.es/sites/default/files/2019-09/guia-privacidad-y-seguridad-en-internet.pdf

[137] POSTALTIC/EP, (19 de noviembre, 2019), Hackean miles de cuentas de Disney+ y sus contraseñas se ponen a la venta en la Dark Web, *Europapress*, recuperado de: https://www.europapress.es/portaltic/ciberseguridad/noticia-hackean-miles-cuentas-disney-contrasenas-ponen-venta-dark-web-20191119133852.html

[138] DONOVAN N., (28 de noviembre, 2019), Netflix 'reactivated' users without permission, *BBC*, Recuperado de: https://www.bbc.com/news/business-50571832.

[139] Softwares creados de forma malintencionada para dañar un sistema informático.

automáticamente Netflix manda una notificación al correo electrónico del usuario. Por lo tanto, se sugiere hacer campañas enfocadas en los siguientes temas, de esta forma, se benefician tanto los clientes como Netflix.

RECOMENDACIONES Y CONCLUSIONES

PRIMERA: Aunque en un inicio las cuentas compartidas no representaban un problema e incluso era algo visto de forma positiva por los directivos de Netflix, con el paso del tiempo ha quedado demostrado, gracias a los reportes financieros trimestrales de Netflix, que se están dejando de percibir ganancias a causa de este fenómeno que ya se considera una problemática real e inminente, pues conforme a lo que señalan diversos estudios, las pérdidas irán creciendo en tanto no se lleven medidas a cabo.

SEGUNDA: El fenómeno de las cuentas compartidas si bien representa ingresos que está dejando de percibir Netflix, también ha encontrado su sustento en la economía colaborativa, misma que ha beneficiado a la empresa por los siguientes motivos: i) ha funcionado como una forma de marketing para dar a conocer el servicio a más personas que, una vez que dejen de compartir la contraseña, se vuelven potenciales clientes; ii) tomando en cuenta que la mayor parte de las personas que comparten contraseñas son *millenials* y *baby boomers*, se puede considerar que, a futuro, cuando estas personas ya no dependan económicamente de sus padres y tengan un sustento propio, muy posiblemente van a convertirse en suscriptores de Netflix; iii) ha permitido que Netflix crezca y llegue a más nichos, incrementando su valor; iv) ha incorporado un nuevo modelo de negocio en el que convergen la televisión, el cine y el internet; y v) al tener una mayor cantidad de usuarios, el algoritmo de las preferencias resulta más exacto y fiable, ofreciéndoles a los usuarios una experiencia más personalizada. No obstante, no por eso se debe de seguir permitiendo que ocurra con total este fenómeno, sino que las medidas a tomar deben ser amigables con los derechos de los usuarios.

TERCERA: La compartición contraseñas es una violación a los términos y condiciones de Netflix, que también constituye una infracción de propiedad intelectual. Si bien podría entablarse un proceso judicial civil y/o mercantil, respectivamente y solicitar la resolución del contrato más el pago de daños y perjuicios, para la vía civil, o indemnización, para la vía mercantil, estas vías no se recomiendan, pues impactarían negativamente en la reputación de Netflix, debido a que ninguna otra plataforma en el mundo ha llevado a cabo un proceso judicial por estos motivos. Esto amedrentaría tanto a las personas que alejaría a los que ya son clientes y a los que pudiesen ser posibles clientes. Asimismo, cabe destacar que no es posible proceder penalmente puesto que en ningún país de la Unión Europea es considerado un delito.

CUARTA: Los términos de uso de Netflix no contienen claramente cuáles son los casos en los que sí está permitida la compartición de cuentas, pues estas únicamente han sido señaladas por los Directivos de forma no oficial, de manera que se propone incluirlos expresamente en una nueva cláusula, y cuya redacción propuesta es la siguiente:

"**5.1.** El Titular de la cuenta únicamente podrá compartir contraseñas con terceras personas en los siguientes casos:

a. Entre las personas que vivan en el mismo hogar, sin importar si son o no familiares, siempre y cuando residan en el mismo lugar.
b. Los padres podrán compartir su cuenta con sus hijos, aunque estos no residan en el mismo lugar que sus padres. Fuera de este caso, Netflix tiene terminantemente prohibido a los suscriptores que compartan sus cuentas y contraseñas con personas que no vivan en el mismo hogar.

En caso de que Netflix detecte que un Titular de la cuenta ha compartido su usuario y contraseña en supuestos distintos a los aquí permitidos, la cuenta será cancelada o bloqueada de forma inmediata."

QUINTA: Al igual que Netflix, no todas las plataformas de su naturaleza han tomado medidas, tales como Apple TV, Amazon Prime Video y Disney+, quienes solo limitan la transmisión simultánea a determinados dispositivos. No obstante, este último lanzó un comunicado en 2019 indicando que colaborará con el ISP Charter para tomar como medida el bloqueo de direcciones IP, sin dar mayores detalles, pero hasta el momento esto no se ha puesto en marcha. En cambio, HBO ya cuenta con una medida, que es la asociación a dispositivos específicos. Por otro lado, se consideró necesario también analizar otras plataformas que no prestan servicios audiovisuales, pero que sí han tomado cartas en el asunto, como es el caso de PlayStation y de Spotify, quienes han optado por la asociación a determinados dispositivos y la geolocalización, respectivamente.

SEXTA: El problema de la compartición de cuentas no puede ni debe tratarse de forma tajante. Sí se deben de tomar medidas, pero estas deben ser las más sutiles y amigables con el público puesto que, si se toman medidas agresivas, se le ahuyentaría, especialmente al público joven, y ese no es el objetivo, sino incentivarlos a que contraten el servicio directamente y proteger sus derechos como consumidores. Además, es menester señalar

que la suscrita es consciente que las medidas y soluciones planteadas en el presente informe no van a erradicar por completo el problema, pero se pretende reducirlo en la medida de lo posible.

Las medidas analizadas fueron: cambio frecuente de contraseña, sistema de autenticación de doble factor, uso de sistemas biométricos, asociación a dispositivos específicos, uso de geolocalización, bloqueo basado en la dirección IP y uso de inteligencia artificial, aprendizaje automático y análisis de comportamiento; de cuyo análisis se concluye lo siguiente:

- Las menos invasivas para los derechos de los usuarios son el cambio frecuente de contraseña y la autenticación de doble factor. La primera incluso es la medida más débil y la menos recomendada, pues varios estudios sugieren que no se lleve a cabo porque representa un problema en el futuro. La segunda ayudaría a mitigar ataques de cibercriminales, pero la desventaja es que resultaría frustrante y haría la experiencia del usuario bastante tediosa, de manera que se recomienda usarla, pero solamente cuando exista una amenaza de riesgo de vulnerabilidad.
- Las más invasivas son la geolocalización, el bloqueo basado en la dirección IP, el uso de datos biométricos, y el uso de inteligencia artificial, en ese orden, por tratar datos de carácter personal.
    - El uso de datos biométricos además trata datos sensibles, y no es recomendable llevarlo a cabo porque al aplicarle el test de necesidad y de proporcionalidad solo cumplió con 1 de los 3 requisitos que exige la normativa.
    - El bloqueo basado en la dirección IP no es posible llevarlo a cabo ya que para que Netflix pueda identificar a quién corresponde las direcciones IP en las que se registre que se accede al servicio y corroborar si es un cliente o no, el operador ISP debe de proporcionarle los datos de los clientes. Sin embargo, existe una prohibición normativa para poder ceder esos datos, ya que únicamente puede proceder mediante una autorización judicial en caso de delitos tipificados como graves. La compartición de cuentas al no ser delito no entra en este supuesto. Además, no se actualiza el supuesto de interés legítimo. Por lo tanto, esta medida está totalmente descartada.
    - La geolocalización es una medida que podría llevarse a cabo porque a pesar de que trata datos personales, si se siguen las medidas indicadas en el epígrafe 5.5.1, se protegerían los derechos de los usuarios. Sin embargo, presenta las

desventajas en los casos de segundas residencias, al irse de vacaciones o en el transporte, dando lugar a falsos positivos.

- La que probablemente sería la medida más eficaz sería el uso de la tecnología de inteligencia artificial a cargo de la empresa. Si bien es una medida intrusiva no solo por manejar grandes cantidades de datos personales de los miles de usuarios de Netflix, sino también porque realiza un perfilado y se toman decisiones automatizadas, sí pasa el test de proporcionalidad. No obstante, con la información que proporciona la empresa en su página web no es claro el funcionamiento del sistema, los datos que se van a tratar, quién sería el responsable y el encargado. De manera que, una vez teniendo la información completa y siguiendo las medidas señaladas en el epígrafe 5.7.1 podría llevarse a cabo, con la salvedad de valorar el coste que implicaría la contratación de dicho servicio.
- Por lo tanto, la medida que se sugiere implementar es la asociación a dispositivos específicos, ya que es una medida que es amigable con los derechos de los usuarios, que es utilizada por otra plataforma y que ha dado resultados en la misma.

  Para ello, se sugiere que el número máximo de dispositivos sean 2, 4 y 8 para los planes Básico, Estándar y Premium, respectivamente.

  También se sugiere informarle al usuario desde la creación de la cuenta el número de dispositivos a los que tiene derecho. Cuando instale la aplicación en el número máximo de dispositivos permitidos, se sugiere hacerle conocimiento de esto. Asimismo, avisar cuando intente instalar la aplicación en algún otro y ya haya excedido el límite, indicándole que, para ello, tendrá que desvincular la aplicación en algún otro.

  Por último, se sugiere hacer los cambios marcados con rojo a la cláusula 4.3 de los Términos de uso, para quedar redactada de la siguiente forma:

"4.3. Puedes ver el contenido de Netflix principalmente dentro del país en el que hayas establecido tu cuenta y solo en las ubicaciones geográficas donde ofrezcamos nuestro servicio y hayamos licenciado dichos contenidos. El contenido disponible para visionado varía en función de la ubicación geográfica y cambia periódicamente. Además, podrás ver el contenido en los dispositivos que tengas vinculados a tu cuenta. El número de dispositivos en los que puedes ver contenidos de forma simultánea, así como la cantidad de dispositivos que puedes vincular a tu cuenta, dependen de tu plan de suscripción y está especificado en la página "Cuenta"."

BIBLIOGRAFÍA

AGENCIA DE LA UNIÓN EUROPEA PARA LA SEGURIDAD CIBERNÉTICA (ENISA), (2016), Guidelines for SMEs on the security of personal data processing, Recuperado de: https://www.enisa.europa.eu/publications/guidelines-for-smes-on-the-security-of-personal-data-processing

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS (2003), Carácter de dato personal de la dirección IP. Informe 327/2003. Recuperado de: https://www.aepd.es/es/documento/2003-0327.pdf

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, (2019), Estudio Fingerprinting o Huella digital del dispositivo. Recuperado de: https://www.aepd.es/sites/default/files/2019-09/estudio-fingerprinting-huella-digital.pdf.

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, (2019), Listas de tipos de tratamientos de datos que requieren evaluación de impacto relativa a protección de datos (art 35.4). Recuperado de: https://www.aepd.es/sites/default/files/2019-09/listas-dpia-es-35-4.pdf

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, (2020), 14 equívocos con relación a la identificación y autenticación biométrica. Recuperado de: https://www.aepd.es/sites/default/files/2020-06/nota-equivocos-biometria.pdf.

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, (2020), Adecuación al RGPD de tratamientos que incorporan Inteligencia Artificial. Una introducción. Recuperado de: https://www.aepd.es/sites/default/files/2020-02/adecuacion-rgpd-ia.pdf.

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS e INSTITUTO NACIONAL DE CIBERSEGURIDAD, Privacidad y Seguridad en Internet. Recuperado de: https://www.aepd.es/sites/default/files/2019-09/guia-privacidad-y-seguridad-en-internet.pdf.

ALCES P. y GREENFIELD M.M, (2010), They Can Do What!? Limitations on the Use of Change-of-Terms Clauses, Faculty Publications, no. 279, pp. 1099-1145. Recuperado de: https://scholarship.law.wm.edu/facpubs/279.

ANDERSON C., (10 de enero, 2004), The Long Tail, *Wired*. Recuperado de: https://www.wired.com/2004/10/tail/

AUTORIDAD HOLANDESA DE PROTECCIÓN DE DATOS, (2011), Report of findings. Official investigation by the CBP into the processing of geolocation data by TomTom N.V. Recuperado de: https://autoriteitpersoonsgegevens.nl/sites/default/files/downloads/mijn_privacy/en_pb_20120112_investigation-tomtom.pdfse almacen

BARRIOS ANDRÉS M. (2020), *Manual de Derecho Digital*, Tirant Lo Blanch, pp. 53-64 y 199-221.

BERCOVITZ ÁLVAREZ G., (2019), Los derechos de explotación. En Bercovitz Rodríguez-Cano R., *Manual de Propiedad Intelectual*, Tirant Lo Blanch, pp. 83-100.

BONMATÍ SÁNCHEZ J. y GONZALO DOMÉNECH J J., (2020), La gestión de riesgos y su encaje legal en la regulación de la inteligencia artificial, En Arrabal Platero P., Doig Díaz Y., et. al. (Coord.), *Era digital, sociedad y derecho,* Tirant Lo Blanch, p. 115-125.

BROOKIN J., (16 de octubre, 2019), Disney Is Finally Taking On Account Sharers, *Wired*. Recuperado de: https://www.wired.com/story/disney-streaming-account-sharing/.

COMISIÓN EUROPEA, ¿Qué son los datos personales? Recuperado de: https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_es

COMISIÓN EUROPEA (2019), Generar confianza en la inteligencia artificial centrada en el ser humano, COM (2019) 168 final. Recuperado de: https://ec.europa.eu/transparency/regdoc/rep/1/2019/ES/COM-2019-168-F1-ES-MAIN-PART-1.PDF

COMISIÓN NACIONAL DE INFORMÁTICA Y DE LAS LIBERTADES (CNIL), (2018), Biométrie dans les smartphones des particuliers: application du cadre de protection des données. Recuperado de: https://www.cnil.fr/fr/biometrie-dans-les-smartphones-des-particuliers-application-du-cadre-de-protection-des-donnees

COMISIÓN NACIONAL DE INFORMÁTICA Y DE LAS LIBERTADES (CNIL), (2018), Biométrie à disposition de particuliers: quels sont les principes à respecter ?.

Recuperado de: https://www.cnil.fr/fr/biometrie-disposition-de-particuliers-quels-sont-les-principes-respecter

COMISIÓN NACIONAL DE INFORMÁTICA Y DE LAS LIBERTADES (CNIL), (2019), Reconnaissance Faciale. Pour un Debat à la Hauteur des Enjeux, pág. 3. Recuperado de: https://www.cnil.fr/sites/default/files/atoms/files/reconnaissance_faciale.pdf

DONOVAN N., (28 de noviembre, 2019), Netflix 'reactivated' users without permission, *BBC*, Recuperado de: https://www.bbc.com/news/business-50571832.

CRANOR L., (02 de marzo, 2016), Time to rethink mandatory password changes, *Federal Trade Commission*, Recuperado de: https://www.ftc.gov/news-events/blogs/techftc/2016/03/time-rethink-mandatory-password-changes.

ENJOY SAFER TECHNOLOGY, Guía de doble autenticación, pág. 5. Recuperado de: https://www.welivesecurity.com/wp-content/uploads/2014/01/guia-autenticacion-eset.pdf.

GOOGLE y HARRIS POLL, (Octubre, 2019), The United States of P@ssw0rd$. Recuperado de: https://storage.googleapis.com/gweb-uniblog-publish-prod/documents/PasswordCheckup-HarrisPoll-InfographicFINAL.pdf

GRASSI P., GARCIA M. y FENTON J., (2017), Digital Identity Guidelines, *National Institute Of Standards and Technology*, NIST Special Publication 800-63-3. Recuperado de: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf.

GRASSI P., FENTON J. y NEWTON E., (2017), Digital Identity Guidelines, *National Institute of Standards and Technology*, NIST Special Publication 800-63B. Recuperado de: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63b.pdf

GRUPO DE TRABAJO DEL ARTÍCULO 29, (2007), Dictamen 4/2007 sobre el concepto de datos personales, pág. 18. Recuperado de: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_es.pdf

GRUPO DE TRABAJO SOBRE PROTECCIÓN DE DATOS DEL ARTÍCULO 29, (2017), Directrices sobre los delegados de protección de datos (DPD), pág. 13. Recuperado de: https://www.aepd.es/sites/default/files/2019-09/wp243rev01-es.pdf.

GRUPO DE TRABAJO SOBRE PROTECCIÓN DE DATOS ESTABLECIDO POR EL ARTÍCULO 29, (2011), Dictamen 13/2011 sobre los servicios de geolocalización en los dispositivos móviles inteligentes. Recuperado de: https://www.apda.ad/sites/default/files/2018-10/wp185_es.pdf

GRUPO DE TRABAJO DE PROTECCIÓN DE DATOS DEL ARTÍCULO 29, (2014), Opinion 9/2014 on the application of Directive 2002/58/EC to device fingerprinting. Recuperado de: https://www.dataprotection.ro/servlet/ViewDocument?id=1089.

GRUPO DE TRABAJO SOBRE PROTECCIÓN DE DATOS DEL ARTÍCULO 29, (2018), Directrices sobre decisiones individuales automatizadas y elaboración de perfiles a los efectos del Reglamento 2016/679. Recuperado de: https://www.aepd.es/sites/default/files/2019-12/wp251rev01-es.pdf

GRUPO DE TRABAJO DEL ARTÍCULO 29, (2018), Directrices sobre el consentimiento en el sentido del Reglamento (UE) 2016/679. Recuperado de https://www.avpd.euskadi.eus/contenidos/informacion/20161118/es_def/adjuntos/wp259rev01__es20180709.pdf.

HEREDIA RUIZ V., (2016), Revolución Netflix: desafíos para la industria audiovisual, *Chasqui, Revista Latinoamericana de Comunicación*, No. 135, pp. 275-295. Recuperado de: https://dialnet.unirioja.es/servlet/articulo?codigo=6109989

INFORMATION COMMISIONER'S OFFICE, (2019), Guide to the General Data Protection Regulation (GDPR), pp. 239-248. Recuperado de: https://ico.org.uk/media/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr-1-0.pdf

INFORMATION COMMISIONER'S OFFICE, (2020), Guidance on AI and data protection, Recuperado de: https://ico.org.uk/for-organisations/guide-to-data-protection/key-data-protection-themes/guidance-on-ai-and-data-protection/

KWESKIN B., (2017), Netflix and No Chill: The Criminal Ramification of Password Sharing, *The Business, Entrepreneurship & Tax Law Review*, volumen 1, pp. 216-248. Recuperado de: http://scholarship.law.missouri.edu/betr/vol1/iss1/9.

MARTÍNEZ MARTÍNEZ R., (2018), Inteligencia artificial, derecho y derechos fundamentales. En Barrio Andrés, M. y Torregrosa Vázquez J. (Coord.), *Sociedad Digital y Derecho*, pp. 259-277.

MCALONE N., (15 de julio, 2016), NETFLIX: You can share your password, as long as you don't sell it, *Business Insider*, Recuperado de: https://www.businessinsider.com/netflix-says-its-ok-to-share-passwords-2016-7?IR=T.

MCDOWELL B., (2019), Three ways in which GDPR impacts authentication, *Computer fraud and security*, pp. 9-12. Recuperado de: https://reader.elsevier.com/reader/sd/pii/S1361372319300193?token=BEFEAFAAFB3B4F7FF76163F79E17F30B95A4C3F8F0DA41E010C906D922287B163B8585D7B3F36E381C654DBB51CB151E

MONTERO PASCUAL J.J., (2017), La regulación de la economía colaborativa, En Montero Pascual J.J. (Coord.), *La regulación de la economía colaborativa*, Tirant Lo Blanch, Valencia, pp. 10-52.

NEIRA E., (2018), Impacto del modelo de Netflix en el consumo cultural en pantallas, *Anuario AC/E 2018 de cultura digital*, Acción Cultural Española, pp. 68-79. Recuperado de: https://www.accioncultural.es/media/2018/ebook/Anuario/5_ElenaNeira.pdf.

NETFLIX INVESTOR RELATIONS (16 octubre, 2019), *Netflix Q3 2019 Earnings Interview* [Archivo de video], Recuperado de https://www.youtube.com/watch?v=NHK51RgeqdY&feature=youtu.be&t=1825.

OFICINA DE SEGURIDAD DEL INTERNAUTA, (27 de febrero, 2019), El factor de autenticación doble y múltiple. Recuperado de: https://www.osi.es/es/actualidad/blog/2019/02/27/el-factor-de-autenticacion-doble-y-multiple.

OJER T. Y CAPAPÉ E., (2012), Nuevos modelos de negocio en la distribución de contenidos audiovisuales: el caso de Netflix, *Revista Comunicación*, no. 10, vol.1., pp. 187-200. Recuperado de http://www.revistacomunicacion.org/pdf/n10/mesa1/015.Nuevos_modelos_de_negocio_en_la_distribucion_de_contenidos_audiovisuales-el_caso_de_Netflix.pdf

PARKS ASSOCIATES, (15 de enero, 2020), Piracy and account sharing cost US pay-TV and OTT operators more than $9 billion in 2019 and forecasted to reach $66 billion worldwide by 2022. Recuperado de: https://www.parksassociates.com/blog/article/pr-01152020.

PETERSON A., (02 de marzo, 2016), Why changing your password regularly may do more harm than good, *Washington Post*. Recuperado de: https://www.washingtonpost.com/news/the-switch/wp/2016/03/02/the-case-against-the-most-annoying-security-measure-virtually-every-workplace-uses/?arc404=true.

PILOÑETA ALONSO L.M., (2020), Contratos Mercantiles, Ed. Tirant Lo Blanch, Valencia, pp. 109-116.

PLATERO ALCÓN A., (2019), La seguridad como elemento clave en el tratamiento de datos personales en Europa: especial referencia al régimen de responsabilidad civil derivado de las brechas de seguridad, *Lex*, No. 23, Año XVII, pp. 55-73. Recuperado de: https://orcid.org/0000-0002-3318-6441

POSTALTIC/EP, (19 de noviembre, 2019), Hackean miles de cuentas de Disney+ y sus contraseñas se ponen a la venta en la Dark Web, *Europapress*, recuperado de: https://www.europapress.es/portaltic/ciberseguridad/noticia-hackean-miles-cuentas-disney-contrasenas-ponen-venta-dark-web-20191119133852.html

RODRÍGUEZ DE LAS HERAS BALLEL T., Terms of Use, Browse-wrap Agreements and Technological Architecture: Spotting Possible Sources of Unconscionability in the Digital Era, *Contratto e impresa. Europa,* vol. 14, pp. 849-869.

ROSENBLANTT S., (22 de octubre, 2015), How to set up two-factor authentication, *The Parallax*, recuperado de: https://the-parallax.com/2015/10/22/how-to-set-up-two-factor-authentication/.

RYYANEN E. L., (2017), Is Your Roommate a Felon? Considering the Effect of Criminalizing Password Sharing in Nosal II, *SMU Science & Technology Law Review*, volumen 20, No. 1, pp. 47-60. Recuperado de: https://scholar.smu.edu/scitech/vol20/iss1/5

SALINAS S., (19 de agosto, 2018), Millennials are going to extreme lengths to share streaming passwords, and companies are missing out on millions, *CNBC*, Recuperado de:

https://www.cnbc.com/2018/08/19/millennials-are-going-to-extreme-lengths-to-share-streaming-passwords-.html

SAMAMEI A.N., (2017), The computer fraud and abuse act: are you still watching?, *Journal of High Technology Law*, Vol. XVIII No. 1, pp. 98-124. Recuperado de: https://cpb-us-e1.wpmucdn.com/sites.suffolk.edu/dist/5/1153/files/2017/12/The-Computer-Fraud-and-Abuse-Act-z3njmm.pdf

SIRI L., (2016), El rol de Netflix en el ecosistema de medios y telecomunicaciones: ¿El fin de la televisión y del cine?, *Hipertextos*, Vol. 4, No. 5, pp. 47-109. Recuperado de: http://revistahipertextos.org/wp-content/uploads/2016/11/El-rol-de-Netflix-en-el-ecosistema-de-medios-y-telecomunicaciones.-Siri.pdf.

SORIA BARTOLOMÉ B., (2017), Aspectos económicos de la economía colaborativa, En Montero Pascual J.J. (Coord.), *La regulación de la economía colaborativa*, Tirant Lo Blanch, Valencia, pp. 53-71.

SOUTHARD L., (28 de enero, 2020), Could streaming giants start to clamp down on password sharing?, *Marketplace*. Recuperado de: https://www.marketplace.org/2020/01/28/could-streaming-giants-start-to-clamp-down-on-password-sharing/

TECH EVENTS, 07 de enero 2016, CES 2016 Netflix Press Conference Reed Hastings Keynote (P1). [Archivo de video]. Recuperado de: https://www.youtube.com/watch?v=XCdrx9TDEaE

TOURIÑO A., (2017), Marco jurídico para las OTT, Brand in Media. La Revolución Over The Top, En Gómez A. y Gavira C. (Coord.), *Andalucía Promoción Audiovisual*, Nº 16 XVI, pp. 137-150.

VIDA FERNÁNDEZ J., (2018), Los retos de la regulación de la inteligencia artificial: algunas aportaciones desde la perspectiva europea. En Barrio Andrés, M. y Torregrosa Vázquez J. (Coord.), *Sociedad Digital y Derecho*, pp. 203-224.

VELASCO SAN PEDRO L. A., (2018), Economía colaborativa, En Barrio Andrés, M. y Torregrosa Vázquez J. (Coord.), *Sociedad Digital y Derecho*, pp. 633-656.

WEBER M., (Junio, 2019), Can I have your password?, *Reuters*. Recuperado de: http://fingfx.thomsonreuters.com/gfx/rngs/USA-TELEVISION-PASSWORDS-POLL/010041YS48H/index.html

JURISPRUDENCIA EUROPEA

Tribunal de Justicia de la Unión Europea, de 24 de noviembre de 2011, asunto C-70/10 Scarlet Extended (Grupo Belgacom) vs Sabam Sase.

Tribunal de Justicia de la Unión Europea, de 19 de octubre de 2016, asunto 582/14 Patrick Breyer vs Alemania.

Tribunal de Justicia de la Unión Europea, de 17 de marzo de 2016, asunto C-99/15.

Tribunal de Justicia de la Unión Europea, de 16 de julio de 2020, asunto C-311/18.

JURISPRUDENCIA ESPAÑOLA

Audiencia Nacional, de 01 de septiembre de 2011, Recurso 625/2011.

Audiencia Provincial de Madrid, de 24 de noviembre de 2015, Recurso 80/2016.

Audiencia Provincial de Madrid, de 15 de abril de 2016, Recurso 154318/2016.

Tribunal Constitucional, de 15 de octubre de 1996, 297/1996.

Tribunal Supremo, de 22 de marzo de 2013, Recurso 1919/2013.

Tribunal Supremo, de 03 de octubre de 2014, Recurso 6153/2011.

JURISPRUDENCIA ESTADOUNIDENSE

Tribunal del Distrito de California, Sentencia de 17 de octubre de 2000, Pollstar vs Gigmania, Expediente CIV-F-00-5671 REC SMS.

Tribunal de Apelaciones del Noveno Circuito, del 05 de julio de 2016, Estados Unidos de América vs David Nosal, Nos. 14-10037 y 14-10275.

PÁGINAS WEB

Apple, https://www.apple.com/legal/internet-services/itunes/es/terms.html

Disney+, https://www.disneyplus.com/es-es/legal/contrato-de-suscripci%C3%B3n

Google, https://maps.google.com/help/terms_maps/

Google, https://policies.google.com/privacy

HBO, https://es.hboespana.com/terms-and-conditions

Netflix, https://help.netflix.com/es-es/node/412

Netflix, https://help.netflix.com/legal/termsofuse

Netflix, https://www.netflix.com/signup/planform

Netflix, https://s22.q4cdn.com/959853165/files/doc_financials/2020/q1/FINAL-Q1-20-Shareholder-Letter.pdf

PlayStation, http://legaldoc.dl.playstation.net/ps3-eula/psn/es_tosua_es.html

PlayStation, https://www.playstation.com/es-es/legal/software-usage-terms/

PlayStation, https://doc.dl.playstation.net/doc/ps4-eula/ps4_eula_es.html

PlayStation, https://www.playstation.com/es-es/get-help/help-library/my-account/device-activation-deactivation/activating-a-playstation-4-system/

Prime video, https://www.primevideo.com/help/ref=atv_hp_cnt?_encoding=UTF8&nodeId=202095500

Spotify, https://www.spotify.com/es/legal/duo/

Spotify, https://www.spotify.com/es/legal/premium-family-terms/

Spotify, https://www.spotify.com/es/legal/privacy-policy/

Spotify, https://www.spotify.com/es/legal/student-discount-terms-and-conditions/

Synamedia, https://www.synamedia.com/video-solutions/video-security/credentials-sharing/

NORMATIVA EUROPEA

Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos

personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE.

NORMATIVA ESPAÑOLA

Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal. BOE No. 281, de 24 de noviembre de 1995.

Ley 7/1998, de 13 de abril, sobre condiciones generales de la contratación. BOE No. 89, de 14 de abril de 1998.

Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico. BOE No. 166, de 12 de julio de 2002.

Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones. BOE No. 251, de 19 de octubre de 2007.

Real Decreto de 24 de julio de 1889 por el que se publica el Código Civil. BOE No. 206, de 25 de julio de 1889.

Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el texto refundido de la Ley de Propiedad Intelectual, regularizando, aclarando y armonizando las disposiciones legales vigentes sobre la materia.

Real Decreto Legislativo 1/2007, de 16 de noviembre, por el que se aprueba el texto refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias. BOE No. 287, de 30 de noviembre de 2007.

NORMATIVA ESTADOUNIDENSE

Ley de Abuso y Fraude Informático

ANEXO 1

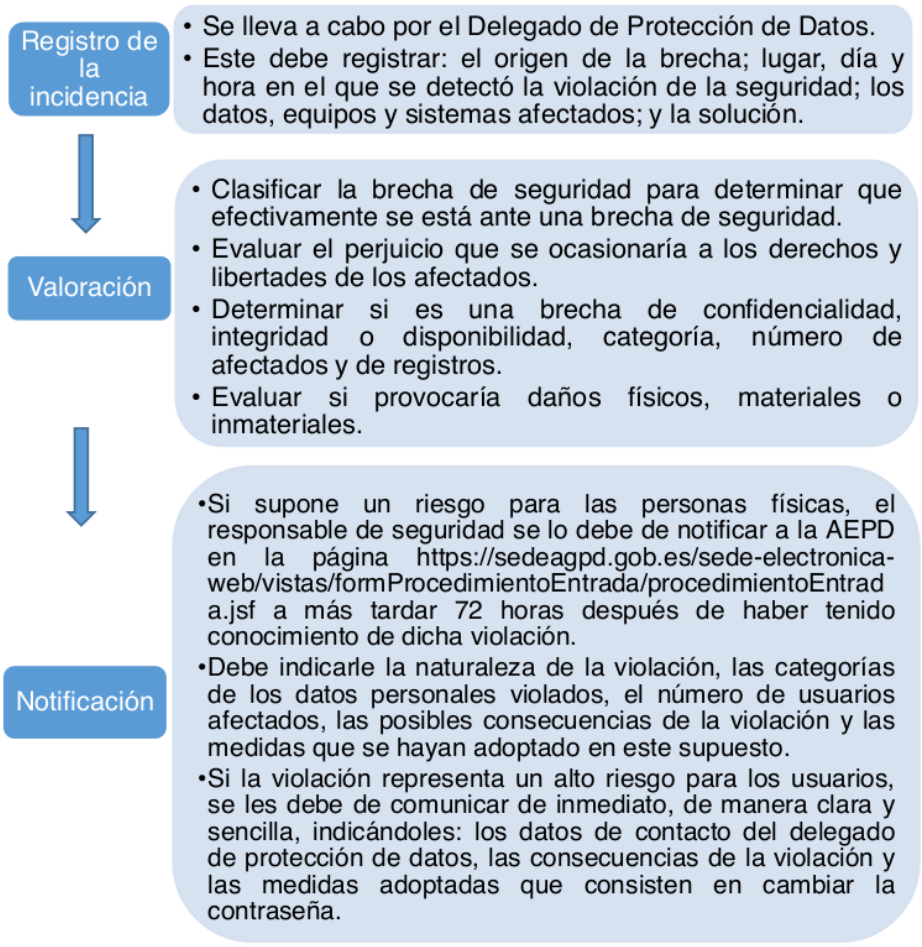
Procedimiento para entablar una demanda vía civil en contra de un usuario

1. Notificarle al usuario que ha incumplido con lo establecido en los Términos de uso de Netflix, por lo que se procederá a resolver el contrato y a solicitar los daños y perjuicios derivados del incumplimiento, vía judicial. Se debe de mandar el mensaje al correo electrónico del usuario con el objeto de probar que efectivamente fue enviado ese mensaje.
2. Entablar una demanda vía civil solicitando la resolución del contrato más el pago de daños y perjuicios y presentándose vía electrónica
    a. Netflix debe demostrar que efectivamente el usuario incumplió el contrato y que hay dolo, es decir, que el usuario actuó con conocimiento de causa de lo que estaba haciendo. Aquí no cabe alegar la culpa pues la intención se muestra desde el momento en el que se comparte la contraseña con alguien más, a sabiendas que está prohibido expresamente, conforme a la propuesta de redacción de la cláusula 5.1.
    b. Es necesario realizar un peritaje con el objeto de calcular los daños y perjuicios ocasionados a Netflix; dependiendo del monto se procede de la siguiente forma:
        i. Juicio verbal. Este procede cuando los daños no superan los 6 mil euros.
            1. Se admite la demanda.
            2. Se le da traslado al demandado.
            3. Contestación de la demanda.
            4. El demandado y el demandante deben indicar si consideran que se celebre la vista.
            5. Si ninguna parte la solicita, se dicta sentencia.
            6. Si se celebra la vista se dicta sentencia dentro de los 10 días.
        ii. Procedimiento ordinario. Procede cuanto la cuantía de los daños es superior a los 6 mil euros.
            1. Se admite la demanda.
            2. Una vez admitida la demanda, se le dará traslado al usuario para que contesten la demanda en 20 días.

3. Contestación de la demanda.
4. Celebración de audiencia previa con el objeto de llegar a un acuerdo sobre el monto de los daños y perjuicios. Si llegan a un acuerdo, ahí termina todo.
5. Si no llegan a un acuerdo, se continúa el proceso y viene la etapa de pruebas.
6. Una vez terminado el juicio de pruebas, se dicta sentencia en un plazo de 20 días.

ANEXO 2

Procedimiento en caso de existir una violación a la seguridad de los datos personales



ANEXO 3

Medidas que se deben de tomar para el uso de datos biométricos

1. La coincidencia y el almacenamiento de los datos biométricos debe quedarse en el dispositivo y no en los servidores, de esta forma se almacenarían en una especie de caja hermética.
2. Se sugiere que los datos queden bajo el control de los usuarios pues esto limitaría los riesgos de procesamiento. Si se tiene una base de datos general, en caso de verse afectada la seguridad, se afectarían los datos de cientos de miles de usuarios. En cambio, al ser de control personal, se afectarían solo los datos de sus titulares.
3. Deber de información. Se debe de comunicar a los titulares de los datos, a través de la Política de Privacidad, lo siguiente:
    a. Características del tratamiento.
    b. Medios para ejercer sus derechos.
    c. Tipos de datos biométricos que se recaban, en este caso, la huella dactilar.
    d. La finalidad del tratamiento.
    e. Si se transfieren o no los datos a terceros.
4. Obtención de consentimiento expreso de los usuarios. De forma informada, específica e inequívoca. Esto es independiente al que se obtiene en los Términos de Uso, puesto que se trata de una finalidad distinta. En este apartado, atendiendo al principio de transparencia, es importante darle a conocer al usuario los datos que se van a tratar, la finalidad y el tiempo en el que se van a recabar los datos.
5. Deber de confidencialidad.
    a. Guardar el secreto del tratamiento en todo el ciclo de los datos.
    b. Verificar que los encargados cumplan con este deber.
    c. Establecer mecanismos para asegurarse que las personas que intervienen en el tratamiento de los datos cumplan con este deber.
    d. No difundir los datos sin el consentimiento del titular.
    e. Especificar las personas que van a estar involucradas en el ciclo de los datos.
6. Nombrar un Delegado de Protección de Datos. Esto es así, ya que se tratan a gran escala datos personales sensibles, como son los datos biométricos, conforme al artículo 37.1 letras b) y c) del RGPD.

7. Análisis de Riesgos, en el que muy probablemente el resultado será que el resultado es alto. Además, es necesario demostrar la responsabilidad proactiva desde el diseño y por defecto.
8. La Evaluación de Impacto se debe realizar por lo siguiente:
    a. El tratamiento de datos personales sensibles, como lo son los datos biométricos, supone un alto riesgo, máxime cuando se utilizan tecnologías innovadoras.
    b. Se tratan datos a gran escala, pues Netflix cuenta con decenas de miles de usuarios a nivel España.

8.1 Asimismo, la Evaluación de Impacto debe contener:

a. Evaluación de la necesidad del tratamiento. Si los datos biométricos son necesarios y efectivos para atender la problemática.
b. Comparar el beneficio que obtendría Netflix versus los costes por posibles violaciones a las normas.
c. Evaluar los riesgos inherentes para los derechos de los usuarios.
d. Evaluar las medidas que se tomarían para mitigar estos riesgos, las cuales deben garantizar un nivel de seguridad adecuado. Una medida que se toma para mitigar los riesgos consiste en procesar los datos biométricos en los dispositivos de los usuarios en lugar de en la nube.
e. Registro de las actividades del tratamiento.
    - Nombre y datos del responsable.
    - Fines del tratamiento.
    - Categorías de los interesados y de los datos personales.
    - Categorías de datos que se comunicarán a terceros (si aplica).
    - Plazos de supresión para las categorías de los datos.

ANEXO 4

Ciclo genérico para realización de Evaluación de Impacto [140]

[140] GRUPO "PROTECCIÓN DE DATOS" DEL ARTÍCULO 29, (2017), Directrices sobre la evaluación de impacto relativa a la protección de datos (EIPD) y para determinar si el tratamiento «entraña probablemente un alto riesgo» a efectos del Reglamento (UE) 2016/679, pág. 18. Recuperado de: https://www.aepd.es/sites/default/files/2019-09/wp248rev01-es.pdf

ANEXO 5

Obligaciones y medidas a tomar en cuenta para el uso de inteligencia artificial, aprendizaje automático y análisis de comportamiento

1. El sistema de Synamedia debe de respetar la dignidad humana, la libertad y los derechos humanos de los usuarios. Además, debe estar adecuado a la normativa europea y debe respetar los principios éticos.
2. Es importante asegurarse que el sistema de Synamedia cumple con los siete requisitos esenciales establecidos por la Comisión Europea:
   a. Sea intervenido y supervisado por los humanos.
      - Al tomar en cuenta que lo primordial debe ser el bienestar del usuario, la intervención humana va a garantizar que el sistema no afecta la autonomía humana ni causará otros efectos negativos.
      - Esto también condiciona a que se cuenten con las adecuadas medidas de control, tales como la adaptabilidad, la exactitud y la explicabilidad.
      - Corroborar que la supervisión sea mediante participación, supervisión o control humanos.
   b. Tenga solidez y seguridad técnicas.
      - Los algoritmos deben ser seguros, fiables y sólidos para poder solucionar cualquier error que hubiese.
      - El sistema debe de ser fiable, resiliente y contar con un plan de contingencia.
      - Integrar mecanismos de seguridad desde el diseño.
      - Debe tener instaurados procesos para evaluar los riesgos.
   c. Prime la privacidad y gestión de datos recabados en todas las fases.
      - Garantizar que los usuarios tienen pleno control de sus datos.
      - Garantizar la integridad de los datos.
      - El acceso a los datos debe estar controlado y regulado.
   d. Transparencia.
      - Garantizar la trazabilidad del sistema.
      - Aportar la explicación del sistema.
      - Comunicar las capacidades y limitaciones del sistema.
      - Debe ser identificables, de manera que los usuarios sepan que están interactuando con un servicio de inteligencia artificial proporcionado por Synamedia a Netflix.

e. Cumpla con la diversidad, no discriminación y equidad.
f. Cumpla con el bienestar social.
g. Rinda cuentas a Netflix.
    - Debe contar con mecanismos que garanticen la rendición de cuentas y sus resultados.
    - Netflix debe de tener la posibilidad de auditar el sistema, ya sea con equipo propio o con algún tercero.
    - Se le debe informar a Netflix acerca de los posibles impactos negativos que pudiese tener el sistema.
    - Synamedia debe garantizar que reparará adecuadamente el sistema en caso de que se produzcan efectos adversos.

3. Evaluar las soluciones del sistema. Para esto, debe de haber parámetros que deben de especificarse:
    a. Precisión, exactitud o medidas de error que se requieran para el tratamiento.
    b. Los datos deben tener buena calidad.
    c. Predictibilidad del algoritmo.
4. En las etapas del ciclo de vida del sistema se pueden tratar datos personales. Para interés de Netflix, se deben de tomar en cuentas las siguientes etapas, entre las que hay que distinguir quién es el responsable y quién es el encargado para efectos de determinar las obligaciones:
    a. Despliegue. En caso de que Synamedia sea un componente, se considera que existe comunicación de datos personales cuando la solución incluye dichos datos personales o hay una forma de obtenerlos.
        - Responsable. En caso de que la solución del sistema sea un componente o esté incluido como parte de la aplicación de Netflix, e incluya datos de carácter personal, se considera que tanto Synamedia como Netflix se comunican los datos personales entre sí, por lo que ambos son responsables.
        - Encargado. Synamedia actuaría como encargado en caso de que ponga a disposición de Netflix el sistema, para que Netflix explote su aplicación, puesto que Synamedia no interviene en dicha explotación.
    b. Explotación. Es importante identificar y conocer cuáles son las actividades propias de Synamedia y de Netflix, así como determinar cómo dependen uno del

otro, pues en esta etapa se ejecutan como tal las actividades, dentro de las cuales, existe tratamiento de datos en las siguientes:

- Inferencia o perfilado. Los datos de los usuarios se usan para obtener un resultado.
    - Responsable. El que trate los datos de los usuarios con el sistema para fines propios.
    - Encargado. Synamedia actuaría como encargado en caso de que ponga a disposición de Netflix el sistema, para que Netflix explote su aplicación, puesto que Synamedia no interviene en dicha explotación.
- Decisión. Es un típico tratamiento de datos.
    - Responsable. El que tome las decisiones automatizadas sobre los usuarios para fines propios.
    - Encargado. Synamedia actuaría como encargado en caso de que ponga a disposición de Netflix el sistema, para que Netflix explote su aplicación, puesto que Synamedia no interviene en dicha explotación.
- Evolución. Al usar los datos obtenido para mejorar o refinar el sistema, también se están tratando datos personales de los usuarios. Si estos datos los realiza Synamedia, existe una comunicación de datos.
    - Responsable. En los siguientes supuestos: i) El que trata los datos de los usuarios; ii) si quien trata los datos de los usuarios los comunique a un tercero, es responsable cuando no existe relación responsable – encargado; o iii) el que determina la evolución del sistema.
    - Encargado. Si quien trata los datos de los usuarios los comunique a un tercero, este tercero actúa como encargado, siempre y cuando no los trate para sus propios fines.

c. Retirada. Esto ocurre cuando Netflix decida dejar de usar el sistema o cuando el usuario se da de baja del servicio. Cabe destacar en esta parte que el responsable del tratamiento determina los fines de este, y también se encarga de la selección más adecuada de una solución tecnológica.

El responsable del tratamiento debe de atender lo siguiente:

5. Legitimación y limitación del tratamiento.
    a. El primer elemento por tomar en cuenta es la legitimación para el tratamiento, de manera que la base de legitimación para el tratamiento de sus datos personales sería el contrato, es decir, los términos de uso de Netflix, por considerarse necesario para ejecutar dicho contrato y se presten los servicios.
    b. El hecho de tener una base legitimadora no da lugar a que se usen los datos de los usuarios para cualquier fin y en cualquier momento, sino únicamente para los fines previstos expresamente, que es detectar cuando haya uso compartido de contraseñas.
    c. El tratamiento de los datos personales debe ser legal, justo y transparente.
6. Deber de información. Netflix debe informar el tratamiento de los datos de forma clara, visible, accesible, sencilla y transparente, con el objeto de que los usuarios sean conscientes de la interacción que tienen con el sistema y entiendan los resultados.
    a. Para esto es importante saber cuáles son los datos que el sistema recabaría de los usuarios, mismos que se deben de especificar en la Política de Privacidad; se les debe de hacer de conocimiento el sistema implementado; si es Synamedia que trata los datos por cuenta de Netflix también se debe de mencionar esto, así como el fin para el cual se utiliza.
    b. Permitir e informar a los usuarios que ejerciten sus derechos. Se señalan algunas anotaciones especiales:
        - Supresión. Se deben incluir periodos de revisión periódica de los datos y el plazo para suprimirlos. Además, los datos se deben suprimir sin dilación indebida[141] en los siguientes supuestos: i) los datos ya no son necesarios para el fin establecido del uso del sistema; ii) el usuario se oponga al tratamiento; iii) los datos se trataron de forma ilícita; y iv) para cumplir con una obligación legal.
        - Etapa de distribución de la solución del sistema. Si de conformidad con Synamedia, en esta etapa se tratan datos personales, hay que: i) suprimirlos o justificar en caso de que esto sea imposible de hacer; ii) informar esta circunstancia a los usuarios; iii) demostrar que se han llevado a cabo las medidas por defecto y por diseño, especialmente la minimización de los datos; y iv) realizar una evaluación de impacto.

[141] Artículo 17.1 del RGPD.

- Bloqueo. Los datos se conservan fuera del tratamiento, pero aplicando medidas técnicas y organizativas que imposibiliten su tratamiento y su visualización, excepto para ponerlos a disposición de jueces, tribunales, Ministerio Fiscal o cualquier autoridad administrativa que tenga competencia, por lo que se debe de considerar desde el diseño.

c. Toda vez que gracias al sistema se elaborarán perfiles o decisiones automatizadas[142], se le debe de informar al usuario.
   - Hacer mención expresa de esta situación.
   - Informar al usuario que puede oponerse a este tratamiento y las consecuencias de ello.
   - Información significativa de la lógica aplicada[143].
   - Importancia y las consecuencias para el usuario por llevar a cabo esta función.
   - También, se deben documentar las incidencias o los cuestionamientos para poder detectar en qué situaciones se necesita la intervención humana.

7. Transparencia. Este es un aspecto crítico para este sistema.
   a. La información referente al sistema y a su funcionamiento debe de estar disponible fácilmente para los usuarios y redactado de forma clara, sencilla, concisa y fácil de entender.
   b. Debe de contener información veraz y sin que se preste a malas interpretaciones. Para esto, también es importante adoptar medidas para determinar la exactitud y la calidad de la información proporcionada a los usuarios.
   c. Se debe nombrar un Delegado de Protección de Datos para gestionar el canal de información con los usuarios, de manera que exista la posibilidad de que estos obtengan información acerca del sistema directamente del delegado. Esta figura es fundamental para que se garantice el cumplimiento y gestión de riesgos de los derechos y las libertades de los usuarios.[144]

---

[142] Si bien en el RGPD no se establece una prohibición en caso de que los usuarios sean menores, cabe hacer la precisión que, de conformidad con los Términos de Uso de Netflix, ningún titular de la cuenta es menor de edad, no obstante, sí existen usuarios que usan el servicio y son menores de edad, mismos que tienen un perfil especial para menores. En el Considerando 71 se señala que el tratamiento automatizado, incluido la elaboración de perfiles no está permitido para los menores; por no estar prohibido expresamente en el RGPD no se considera de carácter absoluto, siempre y cuando se implementen las medidas y las garantías necesarias.

[143] Artículo 13.2 en relación con el 22 del RGPD.

[144] GRUPO DE TRABAJO SOBRE PROTECCIÓN DE DATOS DEL ARTÍCULO 29, (2017), Directrices sobre los delegados de protección de datos (DPD), pág. 13. Recuperado de: https://www.aepd.es/sites/default/files/2019-09/wp243rev01-es.pdf.

8. Limitación de la finalidad. Los datos se deben usar solo para el fin específico, que es detectar la compartición de cuentas en supuestos no autorizados por Netflix.
9. Minimización de los datos. Para poder llevar a cabo el tratamiento es necesario usar solamente los datos mínimos que se requieran para ello, no más, es decir, que son los adecuados, los pertinentes y los limitados. Por eso es importante conocer cuáles son los datos que recaba el sistema, de conformidad con Synamedia. Sabiendo esto, se debe limitar lo siguiente:
    a. La extensión de las categorías de los datos usadas en todas las fases del sistema, tales como nombre, dirección, etc.
    b. La precisión de la información.
    c. La accesibilidad a los datos al personal del responsable y del encargado.
10. Precisión estadística. Se deben usar los procedimientos matemáticos o estadísticos que sean adecuados para el tratamiento, que garanticen la fidelidad e integridad de que los datos de los usuarios son exactos, por lo que es importante documentar todo.
    a. Se debe de verificar.
    b. Se debe de validar para garantizar que los resultados del sistema cumplen con lo que promete Synamedia.
    c. El sistema debe de ser lo suficientemente preciso con el objeto de que se garantice que los datos personales se procesan de forma legal y justa.
    d. Hay que evitar errores en función de la gravedad y la naturaleza de los riesgos.
    e. Evaluar la efectividad del sistema para hacer predicciones sobre los datos que procesa.
    f. Hay que asegurarse que todas las personas que intervienen en el sistema están cualificadas para desempeñar sus funciones.
11. Limitación del plazo de conservación. Los datos se deben conservar únicamente por el tiempo estrictamente necesario, es decir, durante el tiempo en el que se tenga la calidad de usuario por utilizar el servicio de Netflix.
12. Integridad y confidencialidad. Los datos deben tratarse de tal manera que se garantice la seguridad adecuada de los datos de los usuarios, mediante la aplicación de las medidas técnicas y organizativas más apropiadas.
13. Responsabilidad proactiva. Debe de incorporar garantías más allá de las mínimas para gestionar los riesgos que lleguen a presentarse.
    a. Llevar un registro de las actividades de tratamiento.
    b. Método para gestionar riesgos.

- Realizar un Análisis de riesgos. El objeto es determinar si el tratamiento de los datos de los usuarios tendrá efectos negativos en ellos. Para ello es necesario:
  - Identificar las fuentes y hacer el ciclo de vida: captura de datos, clasificación y almacenamiento, uso y tratamiento, cesión o transferencia a terceros y destrucción.
  - Identificar los datos del tratamiento. ¿Dónde se almacenan? ¿Por cuánto tiempo se almacenan?
  - Elaborar un diagrama de flujo de los datos del tratamiento.
  - Para determinar el nivel de riesgo del sistema se toma en cuenta tanto los riesgos derivados del tratamiento en sí como los riesgos derivados del tratamiento en relación con el contexto social y los efectos colaterales que de esto se deriven.
- Realizar una evaluación de impacto, cuyo ciclo genérico se señala en el Anexo 3. Esta es una herramienta preventiva para considerar por qué y cómo se utiliza el sistema, que permite procesar los datos personales, analizar, evaluar y tratar los riesgos de las actividades de la siguiente manera:
  - Descripción del sistema. Indicar: objetivos, colectivos afectados, roles que intervienen en el sistema. Además, también se debe tomar en cuenta: ¿Cómo se van a recopilar, almacenar y tratar los datos? ¿Cuál será el volumen y variedad de los datos? ¿Cuál es la naturaleza de la relación con los usuarios? y ¿Cuáles son los resultados previstos para la sociedad en general y para Netflix?
  - Evaluación de los riesgos. Analizar las incidencias legales, los riesgos legales y el plan de tratamiento legal.
  - Evaluación de la seguridad, transparencia y fiabilidad por defecto y por diseño:
    - Apreciación de los riesgos.
    - Aplicación de medidas fiables.
    - Medidas que garanticen la transparencia, minimización de los datos y que puedan demostrar que se aplica el principio de responsabilidad proactiva.
    - Evaluar los riesgos que existen hacia los datos personales de los usuarios y determinar cómo se abordará.

- Establecer el impacto que tiene en el uso del sistema, mediante el análisis de proporcionalidad y necesidad:

  ¿Es una medida susceptible de conseguir el objetivo propuesto? Sí.

  ¿Existe otra medida más moderada para conseguir el objetivo con la misma eficacia? Existen otras medidas, pero aparentemente esta medida es la que garantiza una mayor eficacia.

  ¿Es una medida ponderada o equilibrada pues se obtienen más beneficios para el interés general que perjuicios sobre otros bienes en conflicto? Sí.

- Evaluación periódica

- También es importante contar con un método para gestionar los riesgos en el que se apliquen atenuantes y eximentes.
- Otra herramienta muy útil es el estándar ISO 31000 sobre gestión de riesgos, que señala que para seleccionar la medida más apta para el fin establecido por Netflix implica obtener una compensación de los costes y los esfuerzos en función de las ventajas obtenidas, tomando en cuenta los requisitos legales y los riesgos sean severos, pero con baja probabilidad.

14. Seguridad de los datos. Se deben aplicar las medidas técnicas y organizativas que garanticen un nivel de seguridad óptimo para los datos de los usuarios, que se adecuen a los costes de aplicación, la naturaleza, el alcance, el contexto, los fines del tratamiento, la probabilidad y la gravedad de las variables, conforme al resultado del Análisis de Riesgos.
    a. Es importante prestar especial atención a las siguientes amenazas[145]:
        - Vulnerabilidades del software.
        - Existencia de troyanos y puertas traseras.
        - Manipulación del sistema o a los parámetros del modelo.
        - Ataques por *adversarial machine learning*.
        - Ataques por imitación de patrones.
        - Re-identificación de los datos personales.
        - Fraude o engaño al sistema por parte de los usuarios.

[145] AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, (2020), *Op. Cit.*, pág. 42.

- Filtrado a terceros de los resultados del perfilado.
- Pérdida o mal uso de los datos personales.

b. Contar con ficheros logs, que determinen quién y cómo accede a los datos, y que proporcionen la trazabilidad.

c. Notificar las violaciones de seguridad.

15. Auditoría. Esta debe realizarse por un externo o por los mismos Netflix y Synamedia, con el objeto de verificar que se cumple la normativa. Se debe realizar durante todo el ciclo de vida del sistema y de los datos, incluyendo su retirada y se deben de revisar todos los puntos anteriores.
16. Transferencias internacionales. Los flujos transfronterizos a terceros países fuera del Espacio Común Europeo deben de contar con las garantías para que las transferencias se realicen con fluidez, mediante la adopción de alguna de las siguientes garantías: Normas corporativas vinculantes, cláusulas tipo adoptadas por la Comisión Europea, cláusulas tipo adoptadas por alguna autoridad de control y aprobadas por la Comisión Europea, códigos de conducta, mecanismos de certificación.

El *Privacy Shield* ya no es válido,[146] por lo que, en ausencia de cualquiera de las garantías señaladas, se sugiere obtener el consentimiento expreso de los usuarios para la realización de las transferencias internacionales, indicándole al usuario el país al que se transfiere y haciéndole de su conocimiento que dicho país no garantiza que sus datos sean tratados conforme a la normativa de la Unión Europea.

[146] Tribunal de Justicia de la Unión Europea, de 6 de julio de 2020, asunto C-311/18.