IUS ET SCIENTIA
2021 • Vol. 7 • Nº 1• ISSN 2444-8478
https://editorial.us.es/es/revistas/ius-et-scientia
https://dx.doi.org/10.12795/IETSCIENTIA • © Editorial Universidad de Sevilla 2021


# Breves notas sobre el régimen de responsabilidad civil derivado de los sistemas de inteligencia artificial: especial referencia al algoritmo de recomendaciones de Netflix

## BRIEF NOTES ON THE CIVIL LIABILITY REGIME DERIVED FROM ARTIFICIAL INTELLIGENCE SYSTEMS: SPECIAL REFERENCE TO THE NETFLIX RECOMMENDATION ALGORITHM

**Alejandro Platero Alcón**
Profesor Derecho Civil
Universidad de Extremadura
platero@unex.es 0000-0002-3318-6441

Recibido: 28 de abril 2021 | Aceptado: 03 de junio 2021

**RESUMEN**

En el presente trabajo se analizarán los postulados existentes en la Unión Europea en relación con el régimen de responsabilidad civil derivado de posibles daños producidos por sistemas de inteligencia artificial. Además, se analizará el sistema de recomendaciones de títulos utilizado por Netflix, sistema que será catalogado como de bajo riesgo, exponiendo también, las posibles consecuencias civiles derivadas del acceso a los datos personales del usuario de la citada plataforma.

**PALABRAS CLAVE**

Inteligencia artificial
Machine learning
Responsabilidad civil
Netflix

**ABSTRACT**

In this paper, the existing regime in the European Union will be analyzed in relation to the civil liability regime, derived from possible damages produced by artificial intelligence systems. In addition, the title recommendation system used by Netflix will be analyzed, a system that will be classified as low risk, also exposing the possible civil consequences derived from accessing the personal data of the user of the aforementioned platform.

**KEYWORDS**

Artificial intelligence
Machine learning
Liability
Netflix

## I. Consideraciones introductorias

¿Quién no ha soñado alguna vez con viajar al futuro? Posiblemente gran parte de los niños de hace unos 30 años, ni en sus mejores sueños se hubieran imaginado con poder tener algún aparato en el bolsillo de su pantalón, con que el poder ver películas, consultar el tiempo, chatear en directo y de inmediato con cualquier otra persona del mundo y, ni que decir tiene, del chiquillo que se hubiera imaginado montando en un coche que pudiera ir de un punto a otro, sin necesidad de que nadie lo condujera, éste último, era un auténtico soñador.

El siglo XXI ha traído consigo, gran cantidad de esos citados sueños y, muchos más, ya que, las tecnologías basadas en sistemas de inteligencia artificial están provocando en la actualidad, un desarrollo tecnológico que, parece no contar con límites. Los citados sistemas de inteligencia artificial se nutren en un primer lugar de datos, en gran medida personales de sus usuarios, por lo que, en su funcionamiento, también deberán tener en cuenta, aparte de cuestionamientos éticos, distintas ramas del ordenamiento jurídico, como es la derivada de la regulación del derecho fundamental de protección de datos personales.

En el presente trabajo, se analizará un aspecto básico en la actividad de cualquier ente, su posible responsabilidad, en este caso, civil. En efecto, existe en la actualidad un interesante debate sobre aspectos como el otorgamiento de una capacidad jurídica a los sujetos denominados robots o, la distinta forma de responder civilmente en función del riesgo creado por los sistemas de inteligencia artificial, resultando necesario profundizar sobre estos aspectos.



Además, se ha procedido a investigar en relación al sistema de recomendaciones de Netflix, una plataforma que utiliza una tecnología que se puede catalogar de bajo riesgo, pero que, para funcionar, almacena una importante cantidad de datos de sus usuarios. Se ha ejercitado el derecho de acceso a los citados datos existentes en Netflix y, se expondrán las consideraciones más importantes al respecto, aludiendo a las posibles consecuencias derivadas de una posible brecha de seguridad en el citado portal.

## II. El auge y repercursiones de la Inteligencia Artificial en europa

### I. Aproximación al complejo entramado jurídico de la IA

En pleno siglo XXI, la sociedad ha evolucionado, quizás hasta límites insospechados hace tan solo 50 años, debido al desarrollo de una tecnología que ha permitido un avance, del que ahora mismo, no se conoce techo o límites (Diamandis y Kotler, 2021). No cabe duda que un papel transcendental en la actualidad, es desarrollado por las tecnologías que emplean en su funcionamiento la conocida, aunque desde un punto de vista técnico en relación con los conocimientos del ser humano mundano, sería mejor denominarla desconocida, inteligencia artificial (en acrónimo IA).

IUS ET SCIENTIA • 2021
Vol. 7 • Nº 1 • pp. 135 - 154
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2021.i01.10

La inteligencia artificial, puede definirse como, "la capacidad de un sistema para interpretar correctamente datos externos, para aprender de dichos datos y emplear esos conocimientos para lograr tareas y metas concretas a través de la adaptación flexible" (Kaplan y Haenlein, 2019, p.17). Se debe precisar que, la inteligencia artificial se encuentra inmersa en muchas actividades cotidianas realizadas por el individuo medio, como cuando introduce una búsqueda en cualquier motor de búsqueda (Moya y Crespo, 2014), o cuando, entre otras, su plataforma audiovisual de cabecera, véase Netflix, por ejemplo, le recomienda una película o serie con un porcentaje de similitud en función de sus gustos.

Sin embargo, existen otras herramientas que se encuentran basadas en la inteligencia artificial que, no se encuentran tal al alcance del ciudadano medio, como la utilizada para la conducción autónoma de vehículos (Danesi, 2018), u otras tecnologías como el desarrollo de aplicaciones para gestionar adecuadamente el tráfico de las ciudades (Eberts y Ventura, 2016). Este último grupo de tecnologías parece evidente, que suponen un mayor riesgo en su uso que, las protagonizadas por ejemplo, por un altavoz inteligente (Corona, 2020) y, por ello, como se expondrá con posterioridad, los actuales informes en materia de responsabilidad civil derivada de los sistemas de inteligencia artificial, dividen a los mismos, en sistemas de alto y bajo riesgo.

Resulta incuestionable que, el uso de las tecnologías basadas en sistemas de inteligencia artificial, supone la asunción de una serie importante de riesgos que, deben ser atendidos por el derecho, como por ejemplo, los que pudiera producir la tecnología que decidiera sobre aspectos médicos de un paciente, la tecnología financiera o bursátil que, decidiera por el ser humano donde invertir en bolsa, por ejemplo, aparte de las ya descritas con anterioridad (Ortega, Gonzalo y Bonmatí, 2021). Y, como no, también deben citarse los daños que pudieran producirse en el derecho fundamental a la protección de datos de los usuarios de las citadas tecnologías, ya que, los citados sistemas de IA, funcionan a partir de la recopilación masiva de datos personales que, deben ser tratados de acuerdo a lo establecido a la normativa comunitaria del citado derecho.



Pero, no solo deben describirse riesgos en el uso y desarrollo de la citada tecnología, sino que como acertadamente advierte la Unión Europea[1] (en acrónimo UE), pueden advertirse una serie de beneficios, ya que:

> "además de aumentar la productividad y la eficiencia, la IA también promete que los seres humanos podrán alcanzar cotas de inteligencia aún ignotas, al facilitar nuevos descubrimientos y ayudar a resolver algunos de los mayores problemas del mundo: desde el tratamiento de enfermedades crónicas, la predicción de brotes de enfermedad o la reducción de las tasas de mortalidad por accidentes de tráfico hasta la lucha contra el cambio climático o la anticipación de las amenazas a la ciberseguridad".(Informe Comisión Europea de 19 febrero 2020).

1. *Informe de la comisión europea sobre las repercusiones en materia de seguridad y responsabilidad civil de la inteligencia artificial, el internet de las cosas y la robótica*, de 19/02/2020, página 3.

IUS ET SCIENTIA • 2021
Vol. 7 • Nº 1 • pp. 135 - 154
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2021.i01.10

## 2. Exposición de los primeros avances en materia de responsabilidad civil

En virtud de lo expuesto con anterioridad, es menester, analizar las repercusiones que desde un punto de civil, pueden provocar los sistemas de IA, es decir, intentar dar luz, a la cuestión sobre la tan temida y necesaria responsabilidad civil. La respuesta a esta cuestión, la debe proporcionar el Derecho, que, aunque puede llegar tarde en la regulación de la inteligencia artificial (Cotino, 2019), pudiera ser que ya tuviera los mimbres adecuados en las anteriores regulaciones para acometer tan compleja empresa, ya que, la doctrina se encuentra dividida en relación a la necesidad de regular un sistema específico en materia de responsabilidad derivada de la IA o, por el contrario, acudir al sistema tradicional de responsabilidad existente en los estados miembros, eso sí, adaptando los mismos a las complejidades técnicas propias de las tecnologías afectadas (Casadedus, 2020).

Lo primero que debe advertirse al respecto, es que, no existe una norma propia de la Unión Europea, en relación el régimen de responsabilidad civil derivado de los sistemas de IA[2], a pesar de que, la Unión lleva preocupándose por la inteligencia artificial desde hace ya tiempo, emitiendo una gran cantidad de documentos, compartiéndose al respecto la idea de que, "se nos hace poco menos que ilusoria compilar y sistematizar, de forma exhaustiva, la ingente cantidad de documentos de diversa índole-directivas, resoluciones, informes, dictámenes, comunicaciones-, emitida por muy distintos órganos e instituciones europeos, sobre cuestiones relacionadas con este tema" (Zurita, 2021, p.40).

A pesar de lo anterior, se va a proceder a exponer las principales ideas contenidas en los documentos de la UE, en relación con la responsabilidad civil derivada de la IA, en orden cronológico, analizando con mayor profundidad en el siguiente apartado, el último de los citados documentos publicado. Así, debe citarse en primer lugar la Resolución del Parlamento Europeo, de 16 de febrero de 2017, con recomendaciones destinadas a la Comisión sobre normas de Derecho civil sobre robótica[3], donde ya se planteaba la necesidad de debatir acerca de la validez de los instrumentos jurídicos existentes para solucionar los posibles problemas de responsabilidad civil o, la necesidad de promulgar un estatuto específico al respecto[4].

Con posterioridad, debe citarse que el 25 de abril de 2018 la Comisión Europea publicaba su Comunicación titulada, Inteligencia artificial para Europa[5], donde ya se apuntaba a la Directiva 85/374/CEE sobre responsabilidad por daños causados por los



2. Afirmación realizada a 30 de abril del año 2021.

3. Resolución del Parlamento Europeo, de 16 de febrero de 2017, con recomendaciones destinadas a la Comisión sobre normas de Derecho civil sobre robótica (2015/2103(INL): Entre otros, ya se advertían de los peligros de los vehículos autónomos, drones o robots médicos.

4. En palabras de Minero Alejandre, G., (2020). Robots y derecho civil. Algunas cuestiones a tener en cuenta desde la perspectiva europea. En I. González Pulido y F. Bueno de mata (Eds), *FODERTICS 8.0: estudios sobre tecnologías disruptivas y justicia* (pp.55-66). Granada: Comares, p. 60: "¿Es la normativa general de los Estados miembros sobre responsabilidad civil y sobre propiedad intelectual, industrial y protección de datos personales suficiente o se requieren normas específicas aplicables a robots?"

5. Comunicación sobre Inteligencia artificial para Europa de 25 de abril de 2018, COM(2018) 237 final.

IUS ET SCIENTIA • 2021
Vol. 7 • Nº 1 • pp. 135 - 154
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2021.i01.10

productos defectuosos[6], como un posible instrumento valido para solucionar aspectos de responsabilidad civil, donde entre otras cuestiones, se establece un sistema objetivo de responsabilidad. Ahora bien, como después se profundizará, la aplicación del citado instrumento puede provocar numerosos problemas jurídicos, sobre todo interpretativos, en relación de que se entiende por producto en la IA y, quien o quienes son considerados productores (García Teruel, 2021).

Resulta interesante nombrar también el informe de 8 de abril de 2019, sobre directrices éticas para una IA fiable, elaborado por un grupo de expertos independientes[7], donde se hacía mención a la posibilidad de crear sellos de certificación de calidad relacionados con el cumplimiento de principios éticos, ahora bien, también se menciona expresamente que aunque el desarrollador de la tecnología posea la citada certificación, no significaría que quedara exento de los daños que se produzcan en materia de responsabilidad civil. Sobre este sistema, debe destacarse que no las certificaciones no podrían ser otorgadas de forma propia, sino que serían auditores externos los que realizaran la citada actividad (Cotino, 2019).

De notable transcendencia es también, el informe de 21 de noviembre de 2019, titulado *Liability for artificial intelligence and other emerginf digital technologies*,[8] publicado por otro grupo de expertos. En el mismo, se vuelve a poner de manifiesto que la normativa sobre productos defectuosos es totalmente valida para exigir una indemnización por posibles daños derivados de accidentes y, se apunta al sistema indemnizatorio de la norma de protección de datos personales europeo, como también posible vía para exigir la reparación del daño causado por los sistemas de IA que, no traten adecuadamente los datos personales de sus usuarios (Gómez y García, 2020). Además, el citado informe comienza una senda de distinción que todavía existe en la actualidad, considerando como responsabilidad objetiva, los daños derivados de IA de alto riesgo, como pudiera ser los de la conducción autónoma, mientras que los daños producidos por la IA de bajo riesgo, como los derivados del algoritmo de preferencias en visualización de Netflix, por ejemplo, serían daños de carácter subjetivos.

Apenas 3 meses después del anterior, se publicó el 19 de febrero de 2020, el Informe de la Comisión sobre las repercusiones en materia de seguridad y responsabilidad civil de la inteligencia artificial, el internet de las cosas y la robótica[9]. De su contenido, debe destacarse la incidencia en la necesidad de alterar la carga de la prueba y, articular



6. Directiva del Consejo, de 25 de julio de 1985, relativa a la aproximación de las disposiciones legales, reglamentarias y administrativas de los Estados miembros en materia de responsabilidad por los daños causados por productos defectuosos, «DOCE» núm. 210, de 7 de agosto de 1985.

7. Informe de 8 de abril de 2019, sobre directrices éticas para una IA fiable. Disponible en: https://op.europa.eu/es/publication-detail/-/publication/d3988569-0434-11ea-8c1f-01aa75ed71a1, (consultado el 30 de abril de 2021).

8. Informe de 21 de noviembre de 2019, titulado *Liability for artificial intelligence and other emerginf digital technologies*. Texto en inglés, disponible en: https://op.europa.eu/es/publication-detail/-/publication/1c5e30be-1197-11ea-8c1f-01aa75ed71a1/language-en/format-PDF#document-info (consultado el 30 de abril de 2021).

9. Informe de la Comisión sobre las repercusiones en materia de seguridad y responsabilidad civil de la inteligencia artificial, el internet de las cosas y la robótica, de 19 de febrero 2020, COM(2020) 64 final.

IUS ET SCIENTIA • 2021
Vol. 7 • Nº 1 • pp. 135 - 154
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2021.i01.10

un sistema de responsabilidad civil que no desproteja al consumidor ante la conocida como brecha de responsabilidad o *responsability gap* (Villar, 2020), debido al efecto de caja negra que se produce en los sistemas de IA, donde el dañado, difícilmente tendrá ni los conocimientos técnicos del funcionamiento de la tecnología ni, tendrá claro ante que sujeto debe reclamar el resarcimiento de daños.

En último lugar, antes de hacer referencia a la situación actual, debe citarse el Libro Blanco de la Unión Europea emitido el día 19 de febrero del año 2020[10]. El citado libro, ha sido considerado como el principal antecedente de la regulación actual europea sobre la IA (Fernández, 2020) y, en concreto sobre el ámbito de la responsabilidad civil, resulta interesante que establece una serie de áreas que deben ser consideradas del alto riesgo, como son la sanidad, el transporte, la energía e incluso, la actividad desarrollada por IA que desarrollen procesos de contratación y, las técnicas de identificación biométrica remota, es decir, aquellas que suponen la identificación de personas en espacio abierto y público.

## 3. Análisis de la resolución más reciente sobre responsabilidad civil e inteligencia artificial

En el presente apartado, se analizarán los más recientes y completos postulados en relación con el régimen de responsabilidad civil, derivados de los sistemas de inteligencia artificial que, se encuentran sintetizados en la Resolución del Parlamento Europeo, de 20 de octubre de 2020, con recomendaciones destinadas a la Comisión sobre un régimen de responsabilidad civil en materia de inteligencia artificial[11], donde se recoge una propuesta de Reglamento al respecto.



Sobre la citada propuesta, debe citarse en primer lugar, el establecimiento en su artículo tercero de un conjunto de conceptos, entre los que se encuentran algunos transcendentes en materia de responsabilidad. Así, se considera de *alto riesgo*, al:

> "potencial significativo en un sistema de IA que funciona de forma autónoma para causar daños o perjuicios a una o más personas de manera aleatoria y que excede lo que cabe esperar razonablemente; la magnitud del potencial depende de la relación entre la gravedad del posible daño o perjuicio, el grado de autonomía de la toma de decisiones, la probabilidad de que el riesgo se materialice y el modo y el contexto en que se utiliza el sistema de IA" (Art. 3 Resolución Parlamento Europeo 20 octubre 2020).

Lo que no aparece, es un concepto sobre IA de bajo riesgo, por lo que habrá que definirla en sentido negativo, es decir, lo que no es tecnología del alto riesgo, lo será de bajo riesgo. Para distinguirlas, se ha utilizado algún interesante símil, considerando que, "una IA débil sabe jugar al ajedrez y, una IA fuerte se plantea que entre el ajedrez y

10. Libro Blanco, sobre la inteligencia artificial - un enfoque europeo orientado a la excelencia y la confianza, COM(2020) 65 final.

11. Resolución del Parlamento Europeo, de 20 de octubre de 2020, con recomendaciones destinadas a la Comisión sobre un régimen de responsabilidad civil en materia de inteligencia artificial, (2020/2014(INL)).

IUS ET SCIENTIA • 2021
Vol. 7 • Nº 1 • pp. 135 - 154
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2021.i01.10

las damas hay cierto parecido" (Zornoza, 2020). Así, sobre los sistemas de alto riesgo, se establece un sistema de responsabilidad civil objetivo, por lo que, no podrán eludir su responsabilidad civil alegando que actuaron con la diligencia debida o que el daño o perjuicio fue causado por una actividad, un dispositivo o un proceso autónomos gobernados por su sistema de IA, salvo que el daño hubiera sido causado por un supuesto de fuerza mayor. De lo anterior se extrae que, el fabricante de un coche autónomo deberá responder siempre que se produzca un daño, salvo que, por ejemplo, el daño se hubiera producido por el impacto de un meteorito. Además, se deberá contar con un seguro de responsabilidad civil en estos supuestos, situación que, aunque con matices, es acogida de forma positiva por la doctrina (Atienza, 2020).

Ahora bien, si se trata de un sistema de IA de bajo riesgo, el sistema de responsabilidad civil que se establece se basa en un sistema de dolo o culpa, es decir, un sistema subjetivo de responsabilidad, como el establecido en el artículo 1902 del Código civil español (en acrónimo CC)[12]. Así, el artículo octavo de la propuesta de Reglamento, establece que el operador se podrá exonerar de la responsabilidad si, el sistema de IA se activó sin su conocimiento, al tiempo que se tomaron todas las medidas razonables y necesarias para evitar dicha activación fuera del control del operador, o se observó la diligencia debida a través de la realización de las siguientes acciones: la selección de un sistema de IA adecuado para las tareas y las capacidades pertinentes, la correcta puesta en funcionamiento del sistema de IA, el control de las actividades y el mantenimiento de la fiabilidad operativa mediante la instalación periódica de todas las actualizaciones disponibles.



De hecho, la actualidad y vigor del sistema establecido en el artículo 1902 y siguientes del CC, no debe ponerse entredicho, ya que, si es perfectamente aplicable a supuestos derivados de las nuevas tecnologías, como por ejemplo, en reclamaciones extracontractuales derivadas de daños producidos como consecuencia de incorrectos tratamientos de datos personales, ¿Por qué no sería aplicable también a daños derivados de sistemas de inteligencia artificial? En este sentido, se ha escrito con brillante acierto que:

> "al final el artículo 1902 permanece inmodificado y sigue siendo tan útil en nuestra sociedad postindustrial como lo fue en la sociedad rural española del último cuarto del siglo XIX, o incluso más útil hoy día, puesto que el número de supuestos en los que resulta de aplicación ha aumentado". (Ataz, 2020, p.332)

Parece lógico y aplaudible, la valentía de instaurar un sistema objetivo de responsabilidad para las tecnologías de alto riesgo y, mantener un sistema subjetivo para los supuestos de baja incidencia, porque, es evidente que, si la navegación aérea constituye una actividad con cierto peligro, también otras, como pudiera ser la conducción autónoma, también lo entrañan. Ahora bien, existen autores que muestran su desacuerdo, considerando que:

12. Artículo 1902 Real Decreto de 24 de julio de 1889 por el que se publica el Código Civil, «Gaceta de Madrid» núm. 206, de 25/07/1889: "El que por acción u omisión causa daño a otro, interviniendo culpa o negligencia, está obligado a reparar el daño causado".

IUS ET SCIENTIA • 2021
Vol. 7 • Nº 1 • pp. 135 - 154
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2021.i01.10

> "ha de partirse de una responsabilidad subjetiva (por culpa) con la aplicación de ciertas teorías (como la inversión de la carga de la prueba) que favorezcan al demandante. No es adecuado considerar que el uso de esta tecnología es, en todos los casos, potencialmente peligroso y apto para producir daños. Muy al contrario, es una herramienta que mejora la vida de las personas y que favorece el desarrollo de la humanidad". (Ortiz, 2021, p.60)

Otro tema interesante, radica en la delimitación del sujeto o sujetos responsables del daño acaecido. En este sentido, debe destacarse que la propuesta de Reglamento no atribuye una *personalidad jurídica* a los propios sistemas de inteligencia artificial, la cual habría supuesto, "una invención puramente técnica, formal y abstracta, con el objeto de proteger determinados intereses de la humanidad, teniendo muy presente su condición de sistema sometido y subordinado en todo momento al beneficio e interés de los humanos" (Azcarate, Ruiz y Amorós, 2020, p. 12).

Sobre la atribución de la citada personalidad jurídica a los robots o determinados sistemas de IA, existe un interesante debate en la doctrina, existiendo autores que incluso presentan propuestas de atribución de la misma en base de cuatro principios bioéticos: beneficencia, no maleficencia, autonomía y justicia (González Granado, 2020), aunque el presente autor considera que, dicha consideración todavía es prematura, ya que, resulta difícil aventurar cuales serán los propios limites legales, que el ser humano imponga a la tecnología.

El sujeto responsable es el operador, tanto inicial como final, ambos siendo definidos. Así, es considerado como operador inicial, "toda persona física o jurídica que define, de forma continuada, las características de la tecnología y proporciona datos y un servicio de apoyo final de base esencial y, por tanto, ejerce también grado de control sobre un riesgo asociado a la operación y el funcionamiento del sistema de IA", mientras que operador final, sería toda persona física o jurídica que ejerce un grado de control sobre un riesgo asociado a la operación y el funcionamiento del sistema de IA y se beneficia de su funcionamiento. Ahora bien, la propia propuesta establece que, si el operador inicial, es también productor en el sentido de lo establecido en la Directiva 85/374/CEE sobre productos defectuosos[13], la normativa aplicable en materia de responsabilidad será la establecida en este último texto legal.

Sobre los daños indemnizables, se identifican daños tanto de carácter material como, de carácter físico, así como daños morales, aunque la cuantía indemnizatoria dependerá de si el sistema de IA es considerado de alto riesgo o no. Además, si el daño se produce en el seno de una relación de carácter contractual, habrá que tener en cuenta, según el artículo cinco de la propuesta de Reglamento que, si es menor de 500 euros, no se articulará la misma bajo lo establecido en ella. Además, en el caso de exista más

13. Artículo 3 Directiva 85/374/CEE sobre productos defectuosos: "se entiende por «productor» la persona que fabrica un producto acabado, que produce una materia prima o que fabrica una parte integrante , y toda aquella persona que se presente como productor poniendo su nombre , marca o cualquier otro signo distintivo en el producto".



IUS ET SCIENTIA • 2021
Vol. 7 • Nº 1 • pp. 135 - 154
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2021.i01.10

de un operador, se establece una presunción de solidaridad, al objeto de beneficiar al sujeto dañado.

Ya, para terminar, se debe hacer una referencia a los plazos de *prescripción*. Así, para los supuestos de daños derivados de IA de bajo riesgo, los plazos serán los establecidos en cada estado miembro, es decir, en el caso español si la responsabilidad tuviera origen en una relación contractual, sería de 5 años, mientras que, si fuera de índole extracontractual, el plazo se reduciría a 1 año. Ahora bien, en este sentido se debe indicar, que cada día se encuentran más difuminados la diferencia entre ambos regímenes y, en especial, al acudir a la teoría de la *estricta orbita de lo pactado*[14], se podrán ocasionar daños encuadrables tanto en un origen contractual o extracontractual. Piénsese, por ejemplo, en daños que se derivan de la filtración de las búsquedas que se realizan en un altavoz digital en un domicilio particular, altavoz que funciona mediante un sistema de IA que, quizás es actualizado y almacenado, por una entidad distinta de la que lo comercializa, ¿Qué existe responsabilidad contractual o extracontractual respecto del dañado? y, por ende, ¿Qué plazo utilizará para reclamar los daños, de 1 o 5 años? La respuesta, desde luego, no es pacífica.

En cambio, si los daños vienen derivados de sistemas de IA de alto riesgo, se establecen en la propuesta de Reglamento, unos plazos propios de prescripción. En efecto, el artículo 7, establece que, en los daños relativos a la vida, la salud o la integridad física el plazo de prescripción será de treinta años a partir de la fecha en que se produjo el daño. Ahora bien, si los daños son materiales o morales, se establece un doble sistema de cuantificación de los plazos de prescripción, escogiéndose aquel que venza en primer lugar, de suerte tal que serán de: a) diez años a partir de la fecha en que se produjo el menoscabo a los bienes o la pérdida económica comprobable resultante del daño moral significativo, respectivamente, o b) treinta años a partir de la fecha en que tuvo lugar la operación del sistema de IA de alto riesgo que causó posteriormente el menoscabo a los bienes o el daño moral.



## III. Consideraciones sobre el sistema de machine learning de netflix

### 1. La compleja política de privacidad de Netflix

Como se ha anunciado anteriormente, se va a analizar en el presente apartado, el funcionamiento del conocido como sistema de recomendación de Netflix, es decir, aquel que permite recomendar al usuario de la plataforma, una serie de películas o series que encajan con su personalidad a un determinado porcentaje, normalmente muy alto. La

14. Sentencia del Tribunal Supremo (Sala de lo Civil) de 22 de diciembre de 2008: *"es aplicable el régimen de responsabilidad extracontractual, aunque exista relación obligatoria previa, cuando el daño no haya sido causado en la estricta órbita de lo pactado por tratarse de daños ajenos a la naturaleza del negocio aunque hayan acaecido en la ejecución del mismo. Por el contrario, es aplicable el régimen contractual cuando en un determinado supuesto de hecho la norma prevé una consecuencia jurídica específica para el incumplimiento de la obligación".*

IUS ET SCIENTIA • 2021
Vol. 7 • Nº 1 • pp. 135 - 154
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2021.i01.10

citada tarea de recomendación constituye un pilar básico en el funcionamiento de la plataforma, porque se estima que, si en 90 segundos un usuario no es convencido de visualizar alguno de sus contenidos, abandona la plataforma (Uman, 2018).

Sobre Netflix, debe advertirse que cuenta con 200 millones de suscriptores en todo el mundo, que pagan alrededor de unos 10 euros mensuales, por lo que, no hace falta ser un experto matemático para comprender la importancia de su negocio, nacido en el año 1997 y, que ha tenido que sortear diversas crisis (Tuñon y Gambari, 2019). Ahora bien, para retener a sus suscriptores, necesita suministrarle el contenido que más les interese y, el mismo, puede ser variado en función del tipo de persona, por ello, la citada entidad debe recopilar una serie de datos del mismo, porque ya se sabe: sin datos no hay inteligencia artificial (Fanni, 2020).

En virtud de lo anterior, resulta necesario exponer que tipos de datos recopila Netflix, con anterioridad a conocer como funciona su algoritmo de predicción de preferencias. Así, de su política de privacidad[15], se obtiene que la plataforma obtiene datos de sus usuarios, de 4 fuentes distintas, a saber:

— *Información suministrada por el propio usuario*: efectivamente, el propio usuario al registrarse, o simplemente por contactar con el servicio de atención al cliente, ya deja un rastro en forma de datos personales que es recopilado por la plataforma, citándose en concreto los siguientes: nombre, dirección de correo electrónico, dirección o código postal, método/s de pago y número de teléfono. Además, si el usuario comenta o valora un determinado contenido, también se utilizará y tratará posteriormente esa información,

— *Información obtenida de manera automática*: en este apartado, se enumeran una serie de datos personales que básicamente, son obtenidos por Netflix, en función de la forma en que el usuario usa la plataforma, donde se incluyen datos como se puede observar, de notable transcendencia, como puede ser la dirección IP[16], la página inmediatamente anterior antes de acceder a ella, o la herramienta tecnológica utilizada para visualizar su contenido. Así, con detalle, se enumeran los siguientes: selección de títulos visualizados, las consultas de búsqueda, etc.; interacciones con los correos electrónicos y SMS, y los mensajes enviados por notificaciones 'push' y nuestros canales de mensajería online; detalles de las interacciones con el servicio de atención al cliente, como la fecha,



15. Actualizada a 1 de enero del año 2021.

16. Recuérdese que, aunque ha existido, sobre todo en los comienzos de la configuración del derecho fundamental a la protección de datos, un interesante debate en relación a la consideración o no de la IP como dato personal, ese debate está superado con creces, considerándose sin ninguna duda como tal. Así, sobre este respecto, obsérvese entre otras, la sentencia del Tribunal Supremo, Sala Tercera, de lo Contencioso-administrativo, de 3 octubre 2014, donde en fundamento jurídico cuarto se establece que: "*No cabe duda que, a partir de la dirección IP puede identificarse directa o indirectamente la identidad del interesado, ya que los proveedores de acceso a internet tienen constancia de los nombres, teléfono y otros datos identificativos de los usuarios a los que han asignado las particulares direcciones IP*".

IUS ET SCIENTIA • 2021
Vol. 7 • Nº 1 • pp. 135 - 154
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2021.i01.10

la hora y el motivo de contactar con nosotros, transcripciones de cualquier conversación por chat, tu número de teléfono y grabaciones de las llamadas; los ID de dispositivos u otros identificadores exclusivos, incluidos los de tus dispositivos de red y los dispositivos compatibles con Netflix conectados a la red Wi-Fi; identificadores de dispositivos que se pueden restablecer (también llamados «identificadores de publicidad»), como los de los dispositivos móviles, tabletas y dispositivos de *streaming* que incluyan dichos identificadores ; características de aparatos y programas informáticos (como el tipo y la configuración), información de conexión (incluido el tipo: Wi-Fi, datos móviles, etc.), estadísticas de vistas de páginas, orígenes de remisiones (las URL de referencia, por ejemplo), dirección IP (que puede indicarnos la ubicación aproximada), navegador e información estándar del registro del servidor web; información obtenida mediante la utilización de cookies, contadores de visitas a la web y otras tecnologías, que incluye datos de publicidad (tales como información sobre la disponibilidad y entrega de anuncios, la URL del sitio, así como la fecha y hora).

— *Información de entidades colaboradoras*: Este apartado resulta interesante, en el sentido que Netflix no detalla quienes son sus entidades colaboradoras, lo que puede implicar importantes repercusiones negativas para el usuario, en el caso, más que probable que, la red de colaboradores sea demasiado extensa. Entre otros, se limitan a citar a los servicios de TV o de Internet, u otros proveedores de dispositivos de *streaming*, operadores de telefonía móvil u otras empresas que cobren las cuotas de los clientes u ofrezcan promociones de prepago del servicio de Netflix; así como los proveedores de plataformas de asistencia por voz que permiten la interacción con nuestro servicio mediante comandos de voz, es decir, los ya citados con anterioridad altavoces inteligentes, que en su funcionamiento y actividad de escucha permanente, puedes producir situaciones difíciles de justificar desde el punto de vista de la privacidad del individuo (Lau, Zimmerman y Schaub, 2018).



Respecto a los posibles datos concretos que tratan por la citada vía, sin repetir algunos de los descritos con anterioridad, destacan: los datos asociados a promociones de prepago, a facturación y a la interfaz de usuario, que respaldan la autenticación del usuario, la experiencia de registro en el servicio de Netflix, el procesamiento de pagos de los colaboradores, y la presentación de contenidos de Netflix a través de partes de las interfaces de usuario de los colaboradores.

— *Información proveniente de otras fuentes*: Se trataría de una especie de cajón de sastre, de nuevo sin identificar con claridad, es decir, no se conocen cuales serían las otras fuentes de las que Netflix podría obtener datos personales sobre sus usuarios. Los datos en concreto que se citan son: ubicación basándose en tu dirección IP con el fin de personalizar el servicio; de los posibles proveedores de seguridad se puede obtener información para proteger los sistemas, impedir los fraudes; los proveedores de servicios de pago pueden proporcionar datos

IUS ET SCIENTIA • 2021
Vol. 7 • Nº 1 • pp. 135 - 154
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2021.i01.10

> de pago o de saldo, o cambios en esos datos; los proveedores de servicios de Internet, se obtienen datos demográficos agregados, basados en intereses y relacionados con la publicidad online y, incluso, de las denominadas por Netflix como "fuentes de dominio público", se obtienen publicaciones no privadas de redes sociales y la información disponible en bases de datos públicas, es decir que, si un usuario de cualquier red social no tiene restringido su acceso solo a las personas que el considere, su actividad en la citada red social también es monitorizada por Netflix, resultando necesario reforzar la importancia de la conocida como *privacy by design* (Aljeraisy , Barati, y Rana, 2020).

Evidentemente, aparte de recopilar los anteriores datos para elaborar un algoritmo que permita predecir los gustos sobre el contenido existente en su catálogo, la compañía también los utiliza para fines publicitarios, es decir, la sociedad ya hace tiempo que superó el debate sobre la rentabilización de los datos, cuanto más sepan de cualquier persona, más ingresos obtendrán (Ballesteros, 2020). De esta forma, Netflix advierte claramente en su política de privacidad que puede establecer anuncios basados en el uso que se lleve a cabo en diversas aplicaciones y sitios web de Internet.

Para ello, tendrán en cuenta el uso del navegador del usuario, mediante las *cookies* y los contadores de visitas y, si se utiliza un dispositivo móvil, una tableta o un dispositivo de *streaming* que incluya un identificador de dispositivo que se puede restablecer (identificador de publicidad), ese identificador también puede servir para estimar los posibles intereses del usuario. Ahora bien, también debe advertirse que, Netflix permite al usuario eliminar las *cookies* publicitarias, mediante un acceso bastante sencillo en su web principal, lo que supone un cumplimiento aplaudible en función de las últimas regulaciones comunitarias existentes sobre las mismas (Delgado, 2020).



En relación al ejercicio de los derechos del usuario, se establecen una serie de disposiciones al respecto. Así, se facilita el derecho al acceso de los datos personales, pudiendo solicitar una copia de los mismos a la compañía que, se compromete a entregártela en un plazo máximo de 30 días, aunque parte de la doctrina se plantea, si no debería existir también un derecho de acceso a los algoritmos utilizados por los sistemas de IA (Nuñez, 2020), como pudiera ser el utilizado por Netflix. Igualmente se informa al usuario de la posibilidad de poder ejercer otros derechos, como el de oposición, limitación o portabilidad, facilitando herramientas para poder ejercitarlos.

Resulta interesante destacar la posibilidad de eliminar la cuenta que ostenta el usuario, ya que, según de lo que se desprende en la política de privacidad, su regulación puede suponer una infracción de los postulados contenidos en el actual Reglamento General de Protección de Datos Personales (en acrónimo RGPD). En efecto, Netflix establece que, al eliminar una cuenta, conservará de forma indefinida en el tiempo una serie de información, que la entidad considera que no permite una identificación personal, como sería un identificador del dispositivo, una dirección de correo electrónico asociada a la cuenta e información sobre los métodos de pago, todo ello, según la plataforma, por cuestiones legales.

La citada conservación ilimitada de esos datos debe considerarse *contraria* a los postulados comunitarios. En efecto, el RGPD menciona hasta en 11 ocasiones el término

IUS ET SCIENTIA • 2021
Vol. 7 • Nº 1 • pp. 135 - 154
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2021.i01.10

"conservación" y, en todas ellas aduce posteriormente la necesidad de que los datos personales de un usuario, deben conservarse únicamente por el periodo que sea estrictamente necesario. Muy ilustrativo al respecto, es el artículo 5.1.e) donde se establece que los datos personales deber ser mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento de los datos personales. Se permite la posibilidad, eso sí, de que los datos personales sean conservados por un periodo más largo, pero únicamente con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, no encontrándose por tanto amparo, a la escasa justificación aportada por Netflix para conservar de forma ilimitada los citados datos, ya que es difícil conocer, a que motivos legales se aferran para realizar la citada operación[17].

En relación a las medidas de seguridad, se aluden a medidas administrativas, lógicas, físicas y de gestión razonables para salvaguardar la información personal contra pérdidas, sustracción o acceso, utilización o modificación no autorizados. Ahora bien, tampoco se menciona expresamente el uso de técnicas tan importantes sobre la materia como la seudonimización o anonimización de datos personales (López y Sánchez, 2020).

En último lugar, se establece una edad mínima de 18 años para darte de alta en la plataforma, aunque no se mencionan procesos para comprobar que esa realidad se produce y, se establece que el responsable del tratamiento de los datos personales es Netflix Servicios de Transmisión España, S.L, lo que supone un importante alivio, ante las dificultades tradicionales de ejercitar los derechos ante entidades sitas en territorios alejados de la frontera del usuario.



## 2. Descripción del funcionamiento de su sistema de recomendaciones

Es el momento de analizar como funciona el sistema de inteligencia artificial utilizado por Netflix para recomendar contenido a sus usuarios. Se debe advertir que, en su propia web, se advierte del que citado sistema está formado por *complejos algoritmos* y, que un algoritmo, puede ser definido como, "un constructo matemático con una estructura de control finita, abstracta y efectiva de acción imperativa para cumplir un propósito dada una serie de criterios" (Hill, 2016, p.39). Resulta evidente que los algoritmos[18], son complejos, ya no solo para el lego en informática, sino que también para los propios expertos, debido a su tremenda opacidad, convirtiéndose en invisibles debajo de un manto interminable de programación informática (Monasterio, 2017).

Los algoritmos son diseñados por personas que los introducen en los sistemas propios de inteligencia artificial, para que, de forma autónoma, puedan realizar una serie

17. En el mismo sentido puede citarse el artículo 15 RGPD, donde en relación al derecho de acceso del interesado se establece que debe informarse de: "de ser posible, el plazo previsto de conservación de los datos personales o, de no ser posible, los criterios utilizados para determinar este plazo".

18. El término algoritmo proviene de Abu Abdulah Mihamad ibn Musa AlKhwarismi, un matemático persa del siglo IX. Sobre sus orígenes, véase la obra de STEINER. C.*, (2012).Automate This: How Algorithms Came To Rule The World*. New York: Portfolio/Penguin.

IUS ET SCIENTIA • 2021
Vol. 7 • Nº 1 • pp. 135 - 154
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2021.i01.10

de funciones. Así, en el caso de un coche autónomo, los mismos provocarían que el vehículo circulara sin conductor, pero el problema, ya no solo desde un punto de responsabilidad civil, sino general, será cuando estos algoritmos fallen, considerándose que la objetividad, "de los algoritmos debe cuestionarse y deben diseñarse e implementarse mecanismos de control jurídico e informático que traten de prevenir y lidiar con los errores y sesgos producidos por los procesos de toma de decisiones automatizadas" (Soriano, 2021, p. 91).

Además, se debe precisar que el sistema de IA de Netflix se encuentra basado en el conocido como *machine learning*, es decir, se podría decir, de una manera un tanto coloquial, que los propios algoritmos están diseñados para seguir captando los gustos de los usuarios y, ofrecer día a día nuevas recomendaciones más adaptadas a la personalidad real del mismo (Suresh, Suneetha Sinha, y Prusty, 2020). La complejidad del citado sistema todavía es mayor desde un punto de vista jurídico, aunque, al tratarse de una inteligencia artificial de bajo riesgo y, debido a la unión contractual existente entre usuario y plataforma como se expuso con anterioridad, los daños que se pudieran producir como consecuencia de la misma, deberían dilucidarse de acuerdo a la normativa de protección de datos, que lleva ya un tiempo, intentando adelantarse a un escenario donde el Big data, es parte básica de casi cualquier actividad tecnológica (Gil, 2017).

¿Qué información suministra Netflix sobre su sistema de recomendación? Pues bien, aducen que se basa en un sistema de probabilidad (% de coincidencia es la fórmula utilizada) calculada en función de una serie de factores, como: las propias interacciones del usuario con la plataforma (historial de visualización); las preferencias de otros usuarios similares en la plataforma, ahora bien, ¿Qué se entiende por usuario similar? De esa cuestión no hay rastro en la web; información de los títulos, como su género, categorías, actores o años de estreno, entre otras.



Aparte de los anteriores condicionantes, el porcentaje de coincidencia también tiene en cuenta: la hora del día en que se utiliza el servicio, quizás las personas con hábitos nocturnos tendrán más tolerancia hacía el cine de terror, quien sabe; el tipo de dispositivo utilizado para ver Netflix y, el tiempo que se pasa en la plataforma. Se afirma expresamente no utilizar ni el atributo edad ni el del género para configurar el sistema algorítmico, hecho que, de ser cierto, es aplaudible.

El sistema de recomendaciones comienza desde cero, es decir, en el proceso de registro del usuario en la plataforma, se le recomienda indicar entre una serie de títulos, cuales son su preferidos, ese es el momento en que el algoritmo, junto con los datos personales que ya conoce del mismo, empieza a recomendar una serie de películas o series en concreto. Ahora bien, a medida que el usuario comience a interaccionar con los títulos, las citadas recomendaciones irán variando, adaptándose al comportamiento descrito con anterioridad.

Además, el orden de un panel de un usuario de Netflix puede ser completamente distinto al de otro, porque las filas de visualización de contenido son totalmente distintas, adaptándose en cada momento en los gustos y preferencias de cada usuario. Básicamente, se podría considerar que el sistema de IA es una especie de batidora que se basa en agitar constantemente datos personales de los usuarios y algoritmos, como

IUS ET SCIENTIA • 2021
Vol. 7 • Nº 1 • pp. 135 - 154
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2021.i01.10

se desprende de las 3 últimas líneas existentes en la web de la plataforma, donde también se observa nítidamente las líneas fundamentales del sistema de aprendizaje automático (Lee y Shin, 2020) o *machine learning,* "nuestros datos, algoritmos y sistemas de computación siguen alimentándose unos a otros para producir recomendaciones actualizadas con el fin de proporcionarte un producto de tu agrado".

Ya para dar por finalizada la presente exposición, debe advertirse que Netflix no solo utiliza sus algoritmos para acertar con el contenido que debe comprar a los tenedores de sus derechos y comercializarlo después, sino que también lo está utilizando con importante éxito, para saltarse ese primer paso y, crear un contenido propio, que no debe comprar a nadie y, poder reproducir y vender a terceros como y cuando quiera (Fernández, Neira, y Clares, 2016).

## 3. Análisis de la posible responsabilidad civil derivada del sistema de IA de Netflix

Como ha quedado expuesto, la propuesta de reglamento de responsabilidad civil derivada de daños producidos por sistemas de IA de 20 de octubre de 2020 establece un régimen diferenciado entre los daños producidos por las tecnologías de alto riesgo y por las producidas por el resto de tecnologías. En el caso expuesto, parece evidente, que el sistema de recomendaciones de Netflix no puede a priori provocar un daño a la vida o a la salud de los usuarios, sino que, más bien, los daños que se pudieran producir vendrán determinados por posibles brechas de seguridad que pudieran provocar, el acceso a los datos personales de los usuarios.



Como es sabido, el régimen existente en la actualidad en relación con las brechas de seguridad es el más completo, desde los orígenes del derecho fundamental a la protección de datos personales, resultando heredero del conocido como deber clásico de seguridad en el tratamiento de datos personales por parte del responsable del mismo (Cumbreras, 2020). Ahora bien, de acuerdo con lo descrito con anterioridad tanto en la propuesta de reglamento analizada, como en el propio RGPD, el responsable podría demostrar que actuó correctamente en su deber de custodio de los datos personales de los usuarios y, por tanto, no responder por la citada filtración.

Para ver que posibles datos podría obtener un pirata informático, el presente autor ha ejercitado su derecho de acceso frente a los datos existentes suyos en el portal de Netflix, quien ha suministrado la información con suma celeridad, todo debe decirse[19]. El conjunto de datos almacenados apenas pesaba 2 megabytes y al descomprimir el archivo, aparecen 11 carpetas, donde se encuentran los datos personales divididos en función de su tipología, por ejemplo, existe una carpeta relativa a los pagos de la cuota mensual, otra con información sobre los dispositivos, otra con el conjunto de direcciones IP, en fin, así hasta llegar hasta 11 carpetas.

19. La solicitud fue ejercida el día 19 de abril de 2021 y, el día 21 ya contaba en el correo electrónico, con un enlace para descargar la misma.

IUS ET SCIENTIA • 2021
Vol. 7 • Nº 1 • pp. 135 - 154
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2021.i01.10

Dentro de cada carpeta, aparecen una serie de archivos Excel, donde se encuentran los datos concretos, eso sí, sin ordenar demasiado. Quizás sorprende la exactitud con la que identifican el modelo de televisión u ordenador utilizado, la exacta identificación de la hora en la que se visualizó cualquier contenido y, como no, la IP de cada una de esas visualizaciones. Por supuesto, la información sobre el número de cuenta concreto, también la disponen, ya que, es el medio asociado de pago de la cuota mensual.

Si esa información fuera filtrada, lo primero que debe producirse es un daño, ya que, sino se produjera un daño, de cualquier tipología, no podría considerarse que el mismo debe ser reparado (Busto, 2020). En el presente caso, resultaría difícil que, por filtrarse, por ejemplo, el listado de películas o vídeos que un usuario visualiza, se pudiera producir un daño[20], ahora bien, distinto es que se filtraran datos bancarios, direcciones IP, o especificaciones de dispositivos que, pueden utilizarse para provocar importantes perjuicios. Si se constatara el mismo y, se superan los en ocasiones gravosos problemas de causalidad, podría empezar a determinarse si existe responsabilidad civil contractual o extracontractual, ya que, en ocasiones la doctrina es reticente a comprender que las violaciones del derecho fundamental a la protección de datos, no siempre tienen un origen extracontractual.

A juicio del presente autor, se trataría de una responsabilidad de carácter contractual, que deberá encajarse dentro de los postulados propios del RGPD, donde no se establecen plazos para la interposición de la demanda. Por tanto, acudiendo al régimen general de responsabilidad civil contractual existente en el Código civil, el plazo de prescripción será de 4 años, en virtud de los establecido en el artículo 1964.2 del citado texto legal.



## IV. Conclusiones

La inteligencia artificial ha llegado para quedarse y, salvo que se pongan limites desde el poder legislativo, su nivel de desarrollo es prácticamente imparable y, nadie podrá atisbar cual será su límite. Ahora bien, uno de los principales problemas que se plantean de su utilización, es sin lugar a duda, la posible responsabilidad civil derivada de daños provocados por sus sistemas.

La Unión Europea lleva ya un tiempo mostrando su preocupación por la incidencia del Derecho Civil en la inteligencia artificial, existiendo interesantes debates en relación con diferentes aspectos, como pudiera ser, el derivado del reconocimiento de capacidad jurídica a los propios sistemas de inteligencia artificial, o como queda

20. La cuestión cambiaría si Netflix ofreciera cine de contenido erótico y, por ejemplo, la filtración afecta a un personaje de interés público. Sólo hay que recordar, el escándalo mediático que se produjo, como consecuencia del "*like*" que suministró la cuenta oficial del papa Francisco a la modelo brasileña Natalia Garibotto, en una publicación donde la citada modelo, aparecía con una vestimenta provocativa. La noticia en cuestión puede verse en: https://www.huffingtonpost.es/entry/el-vaticano-investiga-el-me-gusta-de-la-cuenta-del-papa-en-instagram-a-una-modelo-brasilena_es_5fb7caa5c5b6f6adf949d82c, (fecha de consulta 20 de abril de 2021).

IUS ET SCIENTIA • 2021
Vol. 7 • Nº 1 • pp. 135 - 154
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2021.i01.10

mejor expresado desde un punto de vista figurado, a los robots. Sobre esa cuestión, el presente autor ha manifestado sus dudas al citado reconocimiento, ya que, por mucho de estos sistemas puedan llegar a aprender sin ayuda, alguien los ha tenido que programar para que realicen ciertas funciones, aunque sean las iniciales, resultando engañoso atribuir la citada capacidad jurídica a los robots, ya que, además, el citado reconocimiento no producirá ningún beneficio al dañado, ya que, ¿con que patrimonio propio responderá el robot en cuestión? Aún así, lo cierto es que el devenir tecnológico futuro, provocará que ese debate se avive sin ningún ápice de duda.

En la actualidad parece existir un consenso en establecer dos diferentes sistemas de responder por los daños causados en función de la gravedad del sistema de inteligencia artificial que lo provoque, existiendo, por tanto, tecnologías que son consideradas de alto riesgo. En este grupo, se encontrarán, por ejemplo, los daños producidos por vehículos de conducción autónoma, donde los responsables de la tecnología, tanto el operador inicial, como el final, deberán responder de forma objetiva por el daño causado, salvo que concurran supuestos de fuerza mayor. En cambio, si la tecnología causante del daño no es considerada de alto riesgo, se establece un sistema de responsabilidad subjetiva, donde los operadores podrán demostrar que actuaron con toda la diligencia debida, y eximirse del deber de reparación del daño. Tradicionalmente, para eximir un sujeto de un daño derivado de una posible acción, siempre se ha utilizado el canon del conocido como el buen padre de familia, aunque dicha terminología se encuentra en cuarentena por parte de la doctrina, por la falta de inclusión del género femenino, quizás en el ámbito de la inteligencia artificial, también en el futuro se observe referencias a otros cánones de diligencia debida, como, por ejemplo, la exigida a un *buen programador informático*.



Los sistemas de inteligencia artificial necesitan datos para poder funcionar, por lo que, se debe tener en cuenta la normativa comunitaria sobre protección de datos, en el funcionamiento de los mismos. Además, en ocasiones, se podrán producir daños que, serán más fácil de encuadrar a través de los mecanismos indemnizatorios previstos en la citada normativa que, en la futura regulación específica sobre responsabilidad civil derivada de los sistemas de inteligencia artificial.

Resulta interesante conocer la cantidad de datos que maneja de sus usuarios la plataforma Netflix que, posee un sistema de recomendaciones de películas y series, basada en tecnología *machine learning*. Tras ejercer el derecho de acceso, se ha podido comprobar la cantidad concreta y forma de almacenar los datos de sus usuarios y, salvo pequeñas excepciones, derivadas normalmente de la posible relevancia publica del usuario de la citada plataforma, será complicado que se produzca un daño como consecuencia de una brecha de seguridad en la plataforma. Ahora bien, si se produjera el citado daño, el mismo tendría carácter contractual y, al no contener la regulación comunitaria del derecho fundamental de protección de datos personales un estatuto específico en materia de responsabilidad civil, más allá de los postulados contenidos en su artículo 82, habría que acudir al régimen general sobre responsabilidad civil contractual, contenido en el Código Civil español, para determinar los aspectos principales de la acción a interponer.

IUS ET SCIENTIA • 2021
Vol. 7 • Nº 1 • pp. 135 - 154
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2021.i01.10

## Bibliografía

Aljeraisy, A., Barati, M., y Rana, O., (2020). Privacy Laws and Privacy by Design Schemes for the Internet of Things: A Developer's Perspective. *Hal archives-ouvertes*, (6), 1-36.

Ataz López, J., (2020). Daños causados por las cosas. Una nueva visión a raíz de la robótica y de la inteligencia artificial. En M. Herrador Guardia (Ed.), Derecho *de daños 2020* (317-375). Madrid: Lefebvre.

Atienza Navarro, M.L., (2020). La responsabilidad civil por daños causados por sistemas de inteligencia artificial. En M. Martínez Muñoz (Ed.), *Retos y desafíos del contrato de seguro: del necesario "aggiornamento" a la metamorfosis del contrato*, (1093-1104). Madrid: Thomson Reuters-Civitas.

Azcárate Manchado, M., Ruiz Torres, D., y Amorós, L., (2020). A vueltas con la inteligencia artificial y la responsabilidad civil: ¿Dónde convergen y qué problemática conlleva? *Diario la Ley*, (42), 1-20.

Ballesteros Moffa, L.A., (2020).*Las fronteras de la privacidad. Del conflicto entre seguridad pública y datos personales en una sociedad amenazada y tecnológica*. Granada: Comares.

Busto Lago, J.M., (2020). Protección de datos personales y responsabilidad civil. En M. Herrador Guardia (Ed.), Derecho *de daños 2020* (443-512). Madrid: Lefebvre

Casadesus Ripoll, P., (2020). Inteligencia artificial y responsabilidad civil: perspectivas jurídicas y retos legislativos. *Revista de la Facultad de Derecho de México*, (278), 353-374.

Corona Martínez, D., y Wu, M., (2020). Altavoces inteligentes y robots sociales. *Revista DIM: Didáctica, Innovación y Multimedia*, (38), 2020, (1-9).

Cotino Hueso, L., (2019). Ética en el diseño para el desarrollo de una inteligencia artificial, robótica. *Revista catalana de dret públic*, (58) 29-48.

Riesgos e impactos del Big Data, la inteligencia artificial y la robótica. enfoques, modelos y principios de la respuesta del derecho. *Revista General de Derecho Administrativo*, (50), 1-43.

Cumbreras Amaro, M., (2020). La seguridad de los datos personales y la obligación de notificar las brechas de seguridad. *Revista de Derecho, Empresa y Sociedad (REDS),* (16), 151-162.

Danesi, C., (2018). Daños ocasionados por inteligencia artificial: los vehículos autónomos. En E. Llamas Pombo (Ed.), *Congreso Internacional de Derecho Civil Octavo Centenario de la Universidad de Salamanca: libro de ponencias*, (515-526). Valencia: Tirant lo Blanch.

Delgado Sáez, J., (2020). Cookies y consentimiento. A propósito de la Sentencia del Tribunal de Justicia de la Unión Europea (Gran sala), de 1 de octubre de 2019. *Revista Reflexiones sobre derecho privado patrimonial*, (1), 25-38.

Diamandis, P., y Kotler, S., (2021). *El futuro va más rápido de lo que crees. Cómo la convergencia tecnológica está transformando las empresas, la economía y nuestras vidas*. Bilbao: Universidad de Deusto.

Eberts, M., y Ventura Ventura, J.M.,(2016).La utilización de agentes electrónicos inteligentes en el tráfico jurídico ¿Necesitamos reglas especiales en el Derecho de la responsabilidad civil? *Indret: Revista para el Análisis del Derecho*, (3), 1-22.

Fanni, S., (2020). La inteligencia artificial y el cuerpo humano digital: a la búsqueda del habeas data. *IUS ET SCIENTIA*, (2), 200-224.

Fernández Hernández, C., (2020). La nueva estrategia europea sobre el dato y la inteligencia artificial. Foto fija de un diseño en evolución. *Diario la Ley*, (5), 1-25.

Fernández Manzano, E., Neira, E., y Clares Gavilán, J., (2016). Gestión de datos en el negocio audiovisual: Netflix como estudio de caso. *Revista el profesional de la información,* (4), 568-576.



IUS ET SCIENTIA • 2021
Vol. 7 • N° 1 • pp. 135 - 154
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2021.i01.10

Garcia Teruel, R., (2021). El Derecho de daños ante la inteligencia artificial y el machine learning: una aproximación desde las recomendaciones del Parlamento Europeo y del Grupo de Expertos de la Comisión Europea. En J.A., Cobacho Gómez (Ed.), *Cuestiones clásicas y actuales del derecho de daños. Estudios en Homenaje al Profesor Dr. Roca Guillamón* (1009-1055). Pamplona: Aranzadi.

Gil Sánchez, E., (2017). Aproximación al estudio de las decisiones automatizadas en el seno del Reglamento General Europeo de Protección de Datos a la luz de las tecnologías Big data y de aprendizaje computacional. *Revista española de Transparencia*, (5), 165-179.

Gómez Ligüerre, C., y García Micó, G., (2020). Responsabilidad por daños causados por la Inteligencia Artificial y otras tecnologías emergentes *(Liability for Artificial Intelligence and Other Emerging Technologies*). *Indret: Revista para el análisis del Derecho*, (1), 501-511.

González Granado, J., (2020). *De la persona a la personalidad algorítmica. A propósito de la personalidad jurídica de la inteligencia artificial*. Barcelona: Universitat de Barcelona.

Hill, R., (2016) ¿"What an algorithm is?" *Philosophy and Technology*, (1), 35-59.

Kaplan, A., y Haenlein, M., (2019). Siri, Siri in my hand, who´s the fairest in the land? On the interpretations, ilustrations and implications of artificial intelligence *Business Horizons*, (62), 15-25.

Lau, J., Zimmerman, B., y Schaub, F., (2018). Alexa, Are You Listening? Privacy Perceptions, Concerns and Privacy-seeking Behaviors with Smart Speakers. *Proc. ACM Hum.-Comput. Interact*, (2), 1-12.

Lee, I., y ShiN, J., (2020). Machine learning for enterprises: Applications, algorithm selection, and challenges. *Business Horizons*, (2), 157-170.

López Espí, P., y Sánchez Montero, R., (2020). Comentarios sobre la introducción al hash como técnica de seudonimización de datos personales de la AEPD. *Ley privacidad*, (5), 2020, 1-28.

Minero Alejandre, G., (2020). Robots y derecho civil. Algunas cuestiones a tener en cuenta desde la perspectiva europea. En I. González Pulido y F. Bueno de mata (Eds), *FODERTICS 8.0: estudios sobre tecnologías disruptivas y justicia* (pp.55-66). Granada: Comares.

Monasterio Astobiza, A., (2017). Ética algorítmica: Implicaciones éticas de una sociedad cada vez más gobernada por algoritmos. *Revista Dilemata*, (24), 185-217.

Moya Izquierdo, S., y Crespo Vitorique, I.,(2014). Los motores de búsqueda y el "derecho al olvido". Cuando la tecnología avanza más rápido que el Derecho. *Unión Europea Aranzadi*, (10), 27-37.

Nuñez Seoane, J., (2020). El derecho de la información y acceso al funcionamiento de los algoritmos que tratan datos personales. En A. Huergo Lora (Ed.), *La regulación de los algoritmos* (299-315). Pamplona: Aranzadi.

Ortega Gímenez, A., Gonzalo Domenech, J.J., y Bonmatí Sánchez, J., (2021). La aplicación de la inteligencia artificial y el derecho. La gestión de riesgos como fundamento de la diligencia debida frente a los riesgos de la inteligencia artificial. *CEF Legal: revista práctica de derecho. Comentarios y casos prácticos*, (241), 1-32.

Ortiz Fernández, M., (2021). Reflexiones acerca de la Responsabilidad Civil derivada del Uso de la Inteligencia Artificial: Los "Principios" de la Unión Europea. *Revista de Direito da ULP*, (14), 55-78.

Soriano Arnanz, A., (2021). Decisiones automatizadas: problemas y soluciones jurídicas. más allá de la protección de datos. *Revista de derecho público*, (3), 85-127.



IUS ET SCIENTIA • 2021
Vol. 7 • Nº 1 • pp. 135 - 154
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2021.i01.10

Steiner. C.,(2012). *Automate This: How Algorithms Came To Rule The World*. New York: Portfolio/ Penguin,

Suresh, S., Suneetha V., Sinha, N., y Prusty, S., (2020). Latent Approach in Entertainment Industry Using Machine Learning. *International Research Journal on Advanced Science Hub*, (2), 1-12.

Tuñon, J., y Gambari, A., (2019). El pelotazo de Netflix. Claves de un éxito mundial. *Harvard Deusto business review*, (295), 70-82.

Uman, I., (2018). El Efecto Netflix: cómo los Sistemas de Recomendación transforman las Prácticas de Consumo Cultural y la Industria de Contenidos. *Revista de Cuadernos comunicológicos,* (6), 27-42.

Villar Fuentes, I., (2020).Tratamiento de las consecuencias algorítmicas en la UE. En J. Vásquez Santamaría (Ed.), *Debates contemporáneos del proceso en un mundo que se transforma* (180-198). Medellín: Universidad Católica Luis Amigó.

Zornoza Somolinos, A., (2020). Breves apuntes a la propuesta de reglamento del parlamento europeo sobre responsabilidad civil en materia de inteligencia artificial. *Revista de Derecho, Empresa y Sociedad (REDS)*, (17), 95-101.

Zurita Martín, I., (2021). Las propuestas de reforma legislativa del libro blanco europeo sobre inteligencia artificial en materia de seguridad y responsabilidad civil. *Actualidad jurídica iberoamericana*, (14), 438-487.



IUS ET SCIENTIA • 2021
Vol. 7 • N° 1 • pp. 135 - 154
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2021.i01.10