

El derecho a la autodeterminación informativa. Proyecciones y amenazas en el contexto contemporáneo

The right to informational self-determination: Projections and threats in the contemporary context

Humberto Durán Ponce de León

Ministerio Público-Lima Sur

kato_65_betito@hotmail.com

Recibido: 21.05.25

Aceptado: 07.11.25

Resumen

En el presente artículo el autor razona por los contenidos, alcances y proyecciones de los derechos a las autodeterminaciones informativas, efectuando una revisión de los conceptos, el contenido de dicho derecho, las características y elementos de este derecho. Asimismo, también desarrolla la vinculación con otros Principios, para finalmente efectuar un análisis de aquellas prácticas o situaciones que representan una amenaza a la autodeterminación informativa en el contexto actual.

Palabras clave: Autodeterminación informativa, datos personales, banco de datos, libertad, democracia.

Abstract

In this articles, the authors explores the content, scope, and implications of the right to informational self-determination, reviewing its concepts, content, characteristics, and elements. He also develops its connection with other Principles and finally analyzes those practices or situations that pose a threat to informational self-determination in the current context.

Keyword: Informational self-determination, personal data, database, freedom, democracy.

Introducción

Además de gozar de un relativamente amplio reconocimiento desde que fuera configurado por la jurisprudencia germana, el derecho a las autodeterminaciones informativas que se encontraran investigadas en la Constitución Política 1993 en los siguientes términos:

Artículo 2.- Toda persona tiene derecho:

[...]

6. A que el servicio informático, computarizado, publico y/o privado no suministre información que afectara a las intimidades personales y familiares.

Asimismo, para la defensa de este derecho se ha implementado en el artículo 200 de la Constitución el proceso de Hábeas Data”.

Es así como el “derecho a las autodeterminaciones informativas es la respuesta frente a las apariciones de las tecnologías que permiten la acumulación de informaciones a niveles antes impensables”, lo cual generó una nueva actividad: el control de datos, de modo tal que la información pasó a ser considerada un bien en sí mismo, convirtiéndose posteriormente en un insumo de los procesos generados por las nuevas tecnologías en comunicación. Por tanto, así como se generó un nuevo tipo de escenario, la información personal debía ser necesariamente, protegida frente a un uso indebido o excesivo en el manejo de la información personal.

Ahora bien, a pesar del reconocimiento y protección que la autodeterminación informativa ha recibido tanto en la Constitución Política, el Código Procesal Constitucional y la Ley de Protección de Datos Personales (Ley 29733), existen ciertas cuestiones que necesitan de un mayor debate, así como también a la luz de la realidad del último lustro han aparecido situaciones que ponen en evidencia la necesidad de llevar adelante ciertas específicas innovaciones legales, a efectos de incrementar el nivel de protección de la autodeterminación informativa. Es así como son objetivos del presente trabajo:

- 1.- Efectuar la revisión del concepto y alcances del derecho a las autodeterminaciones informativas, así como de la posición que ocupa en relación a otros derechos que también concurren en el aseguramiento de la posición de los individuos en sociedad, “tales como el derecho a la intimidad, al honor, etc”.
- 2.- Analizar si ciertas prácticas o “actividades en el contexto actual, representan un riesgo o amenaza al ejercicio del derecho a la autodeterminaciones informativas, así como identificar a los ámbitos donde se generan dichos riesgos; a efectos de formular recomendaciones para prevenir la afectación a la autodeterminación informativa”.

Aspectos centrales

I.- El contexto: los riesgos para los datos personales

En sede doctrinaria se ha destacado que la economía de datos ha convertido a la información personal en una mercancía, donde la información personal se convierte en un recurso clave almacenado en bases de datos de grandes corporaciones, atesorándose datos como nombres, direcciones, números de contacto, datos relativos a preferencias ideológicas, hábitos de consumo, estado de salud, etc., favoreciendo la manipulación de las decisiones y comportamientos de las personas (Bonilla 2024: 131-133). En suma, los datos pueden ser empleados tanto por cuestiones de rentabilidad comercial o de contralor político sobre las actividades privadas, existiendo una potencial nocividad de un flujo cibernético indiscriminado de información (Bazán 2005: 88).

De acuerdo a lo señalado: a) Las datos personales se han convertido en insumos tanto para entidades comerciales como estatales; b) A consecuencia de ello, el ámbito personal referenciado en dichos datos, es separado de la persona y es puesto en manos de entidades cuyos fines buscan la manipulación y orientación de las decisiones personales; c) Se instauran así, prácticas explícitamente orientadas al control de la persona mediante la

apropiación de las informaciones personales; d) El “aislamiento de la persona y sus datos personales es una contradicción con los modelos de estados constitucionales y democráticos, en la medida en que los derechos involucrados en los datos, quedan a merced de entidades e intereses ajenos a las realizaciones del estudio de vida individual, y entonces la persona deja de ser el centro de la actividad del Estado y de la sociedad, y pasa a convertirse en un elemento subordinado”.

II.- La autodeterminación informativa

El derecho de “autodeterminaciones informativas consistirán en la facultad del titular de los datos personales, de controlar quien seria el destinatario y el uso que se dará a los mismos, y se ejercen a través de los derechos de accesos, rectificaciones y cancelaciones”. Consiste, por tanto, en el derecho a saber y también a la transparencia del procesamiento de los datos, lo cual además constituye un componente fundamental de la noción de Democracia (Bazán 2005: 111). Asimismo, al permitir un conjunto de facultades, se evidencia una característica relacional, dado que se vincula a la protección de otros derechos constitucionales (Roel, Chocano & Salazar 2025: 172).

La persona no sólo tiene derecho a controlar sus datos personales, sino también a decidir sobre la recopilación, procesamiento, almacenamiento y difusión de los mismos, y se reconoce que el control sobre la propia información es una condición fundamental para la autonomía individual, la libertad de pensamiento y la participación en la vida social (Bonilla 2024: 135). Al fundamentarse los derechos en base a las ideas de autodeterminaciones informáticas y autocontroles de las informaciones personales, también se ha destacado la necesidad de establecer una autoridad de controles autónomos e independientes del Gobierno (Contreras 2020: 114-115). Lo que se busca es proteger a la persona en la totalidad de ámbitos, garantizando la facultad de toda persona de ejercer un control en el registro, uso y revelación de los datos que le conciernen (Eguiguren 2015: 133).

Según las precisiones efectuadas, podemos concluir que:

- a) En la medida en que el itinerario y proyecto de vida se retrata en los datos personales, el control sobre los mismos es el mejor indicativo de la existencia de una auténtica autonomía en la persona, por lo que sólo ella debe ser reconocida como la exclusiva titular de sus datos, con el paralelo reconocimiento de su capacidad de decisión respecto a las recopilaciones, almacenamientos, usos y destinos de su data personal.
- b) Si en la esencia de la democracia está la transparencia y supervisión de los procedimientos mediante los cuales se expresa y despliega la voluntad política, de igual manera cada persona está en la capacidad y posibilidad de ser informada sobre la totalidad de disposiciones y consecuencias del uso y empleo de sus datos personales
- c) Es así como la persona tiene la plena facultad de conocimiento sobre los procedimientos, “decisiones y aplicaciones en relación a sus datos personales, conocimiento necesario para que posteriormente pueda ejercer cualquier decisión, ya sea para autorizar o cancelar el uso de su data personal”.
- d) En la medida en que los datos personales permiten diferenciar los diferentes ámbitos o espacios en los que la persona despliega su proyecto de vida, ello implica que la protección que se debe establecer alrededor de los datos, debe ser lo más plena u omnicomprensiva posible, dadas las múltiples proyecciones tanto en el ámbito personal como social.
- e) Por consiguiente, ninguna esfera de poder -público o privado-, posee legitimidad para imponerle un uso desautorizado o incompatible con los intereses, derechos y proyectos de vida de cada persona. Por tanto, el uso de los datos por cuestiones de orden público, sanidad, emergencias, crisis o situaciones de calamidad, si bien puede conllevar a la exigencia del manejo de los datos personales, sin embargo, no autoriza su uso para finalidades ajenas o contrarias con la razón que motivó su recogida o recopilación.

También encontramos que el “derecho a la autodeterminación informativa posee las siguientes características”: a) Inherente, o sea, inseparable de la

persona; b) *Erga omnes*, esto es, oponible a cualquier persona -pública o privada-; c) Personalísimo, es decir, únicamente el titular está legitimado para su ejercicio; d) Irrenunciable, dado que al ser un derecho fundamental no puede ser objeto de renuncia; e) Imprescriptible, esto es, jamás se cancela su ejercicio; y f) Extrapatrimonial, es decir, no incide sobre aspectos susceptibles de valoración económica (Carlen & González 2022: 451).

Asimismo, en relación a su contenido, el derecho de autodeterminación informativa está integrado por un conjunto de facultades tales como: la de disposición de la información sobre uno mismo; de preservación de la identidad informática, esto es, permitir, controlar o rectificar los datos que individualizan a la persona ante las demás (Ordóñez 2017: 97).

Por su parte, otro sector ha señalado que integran el contenido de este derecho las siguientes facultades: 1) A ser informado de la recopilación de sus datos; 2) A conocer la existencia de ficheros y tratamiento de los datos; 3) Acceder a los mismo para comprobar qué información contienen; 4) A obtener la rectificación de los datos que sean erróneos; 5) A la cancelación de los datos que no deban ser tratados o ya no tengan la calidad que justificó el tratamiento de los mismos; 6) A oponerse al tratamiento de los datos cuando no sea necesario de acuerdo a la ley, el consentimiento, y concurran fundados motivos relativos a la situación personal; 7) A no sufrir perjuicio por decisiones adoptadas a consecuencia de perfiles obtenidos informáticamente; 8) Al resarcimiento por un tratamiento de datos que haya incumplido las condiciones establecidas en la ley; 9) A la protección de instituciones especializadas, específicamente creadas para defender este derecho (Murillo 2007: 20).

III.- La autodeterminación informativa y la libertad

En “sede “doctrinaria se reconoce que mediante los principios de las autodeterminaciones informativas se regulan las tutelas de derecho personal. Es uno de los subprincipios del principio de libertades de voluntad y la libertad de disposiciones de la posesión y propiedad o tutelas de las personalidades según las jurisprudencias hispanas de la intimidades de los individuos””. Este

subprincipio es implícito en el ámbito de los datos personales, por lo que se desprende de disposiciones legales, y en combinación, es un principio expreso cuando se configura como base de la actividad interpretativa que regula las disposiciones de los datos personales, y es un principio inexpresso en la función nomofiláctica de la Corte Suprema y de la función del Tribunal Constitucional, creando nuevos ámbitos de aplicación, integrando disposiciones y creando nuevas normas inderogables (Adinolfi 2007: 6).

Asimismo, se “reconoce “que las libertades informáticas incluyen los derechos de las personas al control del uso de data inserta en programas y comprende la facultad de oponerse a que cierta data personal sea empleada con un fin diferente a aquel legítimos que justificará sus obtenciones. Por tanto, si la libertad informática es reconocida como un derecho fundamental, es porque integra un conjunto de derechos, entre los que se encuentra la intimidad, el honor y el derecho al olvido”” (Caballero 2021: 17).

En el ámbito del Derecho internacional, los adecuados tratamientos de las informaciones personales que abarca a la recogida, uso, acceso, divulgación, transferencia, etc. Es esencial para garantizar la vida privada de las personas, y también se vincula con otros derechos como la igualdad y no discriminación”, dado que revelar una información sensible puede generar un trato segregacionista o el aislamiento de la persona (Sosa 2024: 289).

Además de ello, en el “Derecho europeo se han formulado reglas que deben cumplirse en las recopilaciones y tratamientos de data, a efectos de preservar el derecho a la autodeterminación informativa. Tales reglas son: 1) “Debe existir una relación entre los tratamientos de las datas personales que se pretende y el cumplimiento de una finalidad legítima; 2) La adecuación entre la finalidad e información empleadas. El tratamiento además de necesario también debe ser adecuado o razonable de acuerdo al fin que se pretende alcanzar”; 3) La lealtad en la recogida de datos, esto es, debe existir el consentimiento informado, o la cobertura de una previa autorización legal; 4) La exigencia de calidad de la información existente en el fichero u objeto de tratamiento. Dicha calidad debe ser preservada por quien recoge o utiliza la información, y consiste en la veracidad, exactitud y actualidad de los datos personales; 5) La

cesión de datos sólo debe tener lugar cuando además de mediar el consentimiento de la persona o la autorización legal, se preserve la conexión de la finalidad y la proporción, las que están presentes en el origen de la recopilación de esos datos personales; 6) Se debe promover el respeto a los derechos del interesado, de modo tal que sólo son aceptables las limitaciones señaladas en la ley, y además las mismas deben ser motivadas por quien pretendiera hacerlas efectivas (Murillo 1999: 52-53).

IV.- La autodeterminación informativa en la jurisprudencia

En ““sentencia del 15 de diciembre de 1983 el Tribunal Constitucional alemán precisó los perfiles del derecho de autodeterminación informativa de la siguiente manera”:

- El “derecho a la intimidad constituyen una de las expresiones del derecho a las autodeterminaciones informativas, esto es como las facultades personales de decidir por sí mismas cuando y dentro de que limite procederán a relevar una situación referente a su propias vidas””.
- Es contrario al derecho de autodeterminación informativa un orden social y jurídico en el que el ciudadano ya no pudiera conocer quién, qué, cuando y con qué motivo se sabe algo sobre él, lo que afectaría las posibilidades de desarrollo de la personalidad y también el bien público, dado que la autodeterminación es una condición elemental de funcionamiento de cualquier comunidad fundada en la capacidad de obrar y de cooperación de sus ciudadanos (Bazán 2005: 112).

En sede nacional encontramos que en la sentencia emitida en el Expediente 1797-2002-HD/TC (fundamento 3), se estableció que:

- El derecho a la autodeterminación informativa no se confunde con el derecho a la imagen
- Mediante la autodeterminación informativa garantiza que la persona pueda disponer y controlar los datos que sobre ella se hayan registrado, para preservar su imagen derivada de su inserción en la vida en sociedad.
- Tampoco se confunde con el derecho a la identidad personal.

Asimismo, en la sentencia correspondiente al Expediente 4739-2007-PHD/TC (fundamentos 2 y 3), el máximo intérprete constitucional estableció en relación al derecho a la autodeterminación informativa, lo siguiente:

- “Consiste en facultades de la persona para controlar la información que le concierne, y que está contenidas en registros públicos, privados para hacerte a una posible extralimitación de la misma”.
- “Están ligados a los controles sobre las informaciones, como las autodeterminaciones de la vida íntima afecta a lo personal”.
- “Mediante ella se busca proteger a la persona en sí misma, y no solamente en los derechos que involucran la esfera personalísima. Se protege a la persona en la totalidad de ámbitos, por lo que no es identificable con el derecho a la intimidad. Busca garantizar la facultad de cada persona de poder preservarla ejerciendo un control en el registro, uso y revelación de los datos que le conciernen”.

Las situaciones amenazantes para la autodeterminación informativa

En el último lustro han aparecido tanto en el escenario nacional como internacional situaciones y prácticas que representan al mismo tiempo tanto una amenaza como un desafío para la vigencia del derecho a la autodeterminación informativa. Tales situaciones son las siguientes:

Los sistemas de videovigilancia con identificación facial

Frente a la arremetida de la ola delincencial que asola al país, se ha implementado un sistema de cámaras de videovigilancia con identificación facial, invocando como justificación la prevención y el combate al delito. Sin embargo, ello genera las siguientes situaciones:

1) El sistema de identificación facial debe contar con los datos biométricos únicamente de aquellas personas que son objeto de interés por el sistema judicial o de persecución por las autoridades policiales. La pretensión de almacenamiento en la memoria de dicho sistema de la totalidad de datos biométricos de la población es inconstitucional, en la medida en que el combate al delito no justifica la recogida de datos, almacenamiento ni tratamiento de los

datos de cualquier persona. Aceptar que los sistemas de vigilancia puedan tener almacenados los datos de la población implicaría la instalación de un estado de permanente sospecha o supervisión sobre la ciudadanía, perspectiva que es compatible con el modelo del Estado totalitario o fascista, pero que es opuesto al modelo del Estado democrático.

2) Implementar un sistema de identificación facial puede generar el riesgo de seguimiento y grabación de los actos cotidianos de cada persona, los que además de ser irrelevantes para los fines de persecución del delito, sería una manifestación de abuso o arbitrariedad estatal, en la medida en que no existe disposición de rango constitucional o legal que autorice realizar “*de facto*” un seguimiento o rastreo de las actividades de una persona con ausencia de una orden judicial previamente solicitada por un representante del Ministerio Público.

Esto es, tanto la decisión como el empleo de los medios y equipos en la labor de videovigilancia con un sistema de identificación facial, debe darse en el ámbito jurisdiccional y como parte de un debido procedimiento efectuado por las autoridades y/o funcionarios del Ministerio Público, y siempre y cuando ello haya sido previamente regulado en una ley. Los órganos administrativos de cualquier entidad -pública o privada-, carecen de legitimidad y autorización para crear o establecer *motu proprio*, un registro de datos con los datos biométricos de la población.

Además de ello, cabe señalar que, a la fecha no existe ningún estudio ni investigación que confirme la eficacia de la implementación de los sistemas de cámaras de videovigilancia con identificador facial en la lucha contra la delincuencia. Lo que parece ser cierto es que el nivel y letalidad de la actual ola de criminalidad no han disminuido con la instalación de los sistemas de cámaras de videovigilancia con identificador facial.

El caso canadiense

El año 2022 en un contexto de protestas sociales, el gobierno de Canadá ordenó a las entidades bancarias que no dieran crédito ni pagaran los salarios a los participantes en protestas contra el gobierno. El gobierno canadiense implementó dicha medida basándose en sistemas de identificación de los

manifestantes y sus vehículos, y con ausencia de una previa autorización judicial. Se ordenó la congelación de cuentas bancarias y la cancelación de seguros vehiculares.

Se trató de la implementación de una auténtica “incapacidad financiera” y cuyo desencadenante no fue el incumplimiento de alguna obligación financiera o legal previa, sino la participación en las protestas contra el gobierno.

El caso canadiense resulta aleccionador, por lo siguiente:

- 1) El gobierno hizo uso de los datos personales para identificar a los protestantes contra sus políticas, así como sus centros de trabajo, así como las entidades del sistema bancario mediante el cual se les pagaban sus remuneraciones. Datos clave relativos al domicilio, entidad bancaria donde tenían sus ahorros, la placa de los vehículos, así como el número del seguro y del registro tributario, fueron empleados por el gobierno para llevar adelante una orden ilegítima, en tanto la exigencia de inhabilitación o incapacitación financiera no fue el resultado de una orden judicial que pusiera fin a un procedimiento. Tampoco existió una acusación penal por la comisión de algún delito. Tampoco había mediado el incumplimiento de alguna prestación. En otras palabras, con acudir y formar parte de las protestas, los manifestantes no estaban violando ninguna ley, ni afectaron a algún derecho fundamental.
- 2) La autorización para llevar adelante el congelamiento de los pagos y la suspensión en el otorgamiento de crédito provino de una orden directa del Ejecutivo canadiense, y a su vez dicha orden se originó en la convocatoria a protestas contra el gobierno.

Por consiguiente, este caso muestra los peligros de colocar en manos de la autoridad política la posibilidad de un acceso ilimitado a los datos personales de la ciudadanía. Existe el riesgo evidente de emplear los datos personales para identificar el domicilio, lugar de trabajo, historial de salud, historial financiero, historial de viajes, etc. y emplear ello para iniciar una persecución basada en motivaciones de orden político.

Se trata sin duda, de la instalación de un Estado totalitario, el que merced al control de los datos de los ciudadanos, siempre está en condiciones de llevar adelante actos de amedrentamiento con fines de persecución por motivos políticos.

El caso de la publicidad en plataformas virtuales o redes sociales

Si actualmente existen registros donde las personas pueden inscribirse para no recibir llamadas de publicidad, ello puede ampliarse a las redes sociales y plataformas basadas en internet. Carece de sentido preservar “el derecho a la autodeterminación informativa en las comunicaciones telefónicas”, pero debilitarlo en el contexto de las plataformas y servicios basadas en internet.

Una publicidad basada en la interacción de la persona con las empresas puede resultar en cierto modo, razonable. Pero, una publicidad basada en el acceso, recopilación, procesamiento e interpretación de datos personalísimos tales como estado de salud, orientación sexual, nivel de ingresos, etc. ya no puede ser vista como una interacción, sino como un acto de intrusión.

El escaneo del iris de los ojos

Actualmente se ha difundido la práctica de pagar en criptomonedas a las personas a cambio que permitan que se efectúe el escaneo del iris del ojo. Se trata de un pago para entrar a la identidad biométrica, es decir, al centro mismo de la configuración individual y única de cada persona. En el iris del ojo está la identificación que supera a la huella dactilar.

El problema es que mediante el escaneo del iris del ojo se accede al mundo virtual de las criptomonedas, esto es, se pasa del ámbito de la privacidad o intimidad de la persona, hacia un ámbito público, donde las identidades que posteriormente serán adscrita a bienes o servicios, ya no corresponden a quienes son sus titulares, sino a quienes han comprado la identidad biométrica existente en el iris.

Si uno de los “elementos cruciales en la autodeterminación informativa es el conocimiento del tratamiento y destino de los datos personales, desde dicha perspectiva la venta del iris del ojo es un acto nulo en la medida en que quien vende el iris no conoce la finalidad ni el tratamiento que se dará a sus datos personales, y quien efectúa la compra tampoco informa adecuadamente a las personas el por qué de la compra, ni tampoco explica dónde se almacenarán los datos, ni el destino o uso de los mismos”.

Por tanto, lo “más razonable es establecer la moratoria de dicha práctica por vulneración del derecho a la autodeterminación informativa, el que, como ya hemos comprobado, es un derecho irrenunciable, por lo que quienes hayan efectuado la venta pueden exigir la eliminación de los datos de sus iris de cualquier banco de datos en que hayan sido almacenados”.

Caso “el monedero del ahorro”

En las farmacias se ha instaurado la práctica de ofrecer descuentos por la compra de ciertos medicamentos, y han implementado el llamado “monedero del ahorro”, que no es otra cosa que el registro de la persona en la base de datos de la cadena de farmacia. Lo que ocurre en este caso es que en cada compra se registra la adquisición de medicamentos como parte del tratamiento de una enfermedad, lo cual en manos de una empresa del sector salud, puede constituir un indicador sobre el estado de salud de la persona, información que será relevante cuando se trate de contratar un seguro o acudir a un centro médico.

En este caso, el tipo de “medicamentos adquiridos, así como la frecuencia en la compra, son datos que permiten efectuar un seguimiento del estado de salud del paciente/cliente de la farmacia, información que es relevante cuando dicho paciente intenta contratar con una compañía de seguros, o acude a una clínica privada. Al contar con dicha información la parte que redacta el contrato (la empresa de seguros o la clínica privada) se encuentra en una situación de asimetría favorable a sus intereses, situación que es injusta en la medida en que los datos de adquisiciones de los pacientes, recopilados con la finalidad de ofrecerles descuentos, no pueden ser transferidos ni usados para colocar a los usuarios de los servicios de salud en una situación de inferioridad negocial”.

Caso de los aplicativos yape y plin (billetera electrónica)

El registro de las transacciones mediante los aplicativos de pago yape o plin, no puede ser usado como elemento para construir el historial financiero de una persona, a efectos de evaluar su capacidad de pago o posibilidades de acceder a un crédito. Al tratarse de una modalidad de lo que se conoce como “billetera

electrónica”, el único interesado en el acceso, posesión y control de dichas transacciones es la propia persona.

Conclusiones

1.- El “derecho a la autodeterminación informativa no solamente busca preservar el control de la persona sobre sus datos personales. También constituye una garantía de preservación de una actuación correcta, transparente, sin arbitrariedad ni imposiciones por parte de las entidades de Derecho público o privado, y que como parte de sus actividades, tienen el acceso, manejo y uso de los datos personales”.

2.- La autodeterminación informativa actualmente está bajo amenazas provenientes tanto del Estado como de las corporaciones privadas. En el primer caso, se ha comprobado que algunos Estados han hecho un uso indebido de los datos personales para ejercer vigilancia sobre las personas que se han mostrado críticas u opositoras con ciertas medidas de gobierno. En el segundo caso, las corporaciones han mercantilizado los datos personales convirtiéndolos en insumos de estrategias para las campañas publicitarias, llegando a generar programas encargados de analizar e interpretar los datos personales a efectos de generar estrategias de adhesión e identificación con los productos o servicios de las empresas que las contratan.

3.- En el Perú existe el riesgo de que la implementación de sistemas de identificación facial sea instrumentalizada para recopilar información sobre las actividades cotidianas que realizan los ciudadanos, y que carecen de toda relevancia o interés de injerencia para terceros. Asimismo, efectuar un proceso de recogida de datos personales de millones de ciudadanos con el argumento de ubicar a un grupo que representa aproximadamente solo el 0.0001 % del total de la población, no parece ser un argumento legítimo ni razonable.

4.- Se debe establecer la prohibición de transferencia de los datos personales obtenidos mediante las compras que efectúan los consumidores de las farmacias, boticas y centros de salud, puesto que la adquisición de medicamentos y la frecuencia de las compras constituye un indicativo de la evolución del estado de salud de la persona. Dichos datos no deben ser transferidos a las empresas de seguros o clínicas privadas, puesto que dicha información personal los coloca en una situación de ventaja en la contratación.

5.- Asimismo, debe establecerse la nulidad de todo intento por parte de entidades bancarias y financieras, de usar la información de las transferencias mediante los aplicativos de pago yape, plin o cualquier otro; o para formular un perfil o historial financiero de la persona.

6.- Puede formularse en el sistema jurídico peruano la prohibición de toda transferencia o comunicación de información personal respecto a hábitos de compra en farmacias, restaurantes, clínicas y hospitales, a las empresas de seguros o en el ámbito de la salud o del sector bancario y financiero.

Referencias

- Adinolfi, G. (2007). Autodeterminación informativa, consideraciones acerca de un principio general y un derecho fundamental. *Cuestiones Constitucionales*, (17), 3-29.
<https://www.scielo.org.mx/pdf/cconst/n17/n17a1.pdf>
- Bazán, V. (2005). El hábeas data y el derecho de autodeterminación informativa en perspectiva de derecho comparado. *Estudios Constitucionales*, 3(2), 85-139.
<https://www.redalyc.org/pdf/820/82030204.pdf>
- Bonilla, J. C. (2024). IA y Privacidad: Protegiendo la Autodeterminación Informativa en la Era Digital. *Revista de la Facultad de Derecho de México*, 74(290), 125-148.
<https://www.revistas.unam.mx/index.php/rfdm/article/view/89719>

- Caballero, L. (2021). Cartografía legal de la autodeterminación informativa digital: un derecho de construcción jurisprudencial. UNIVERSITAS. Revista de Filosofía, Derecho y Política, (35), 2-27. <https://e-revistas.uc3m.es/index.php/UNIV/article/view/6189>
- Carlen, S., & González, P. (2022). Derecho a la autodeterminación informativa e Inteligencia Artificial. Ratio Iuris. Revista de Derecho, 10(1), 442-504. <https://publicacionescientificas.uces.edu.ar/index.php/ratioiurisB/article/view/1406>
- Contreras, P. (2020). El derecho a la protección de datos personales y el reconocimiento de la autodeterminación informativa en la Constitución chilena. Estudios Constitucionales, 18(2), 87-120. <https://www.scielo.cl/pdf/estconst/v18n2/0718-5200-estconst-18-02-87.pdf>
- Eguiguren Praeli, F. J. (2015). El derecho a la protección de los datos personales. Algunos temas relevantes de su regulación en el Perú. THEMIS Revista de Derecho, (67), 131-140. <https://revistas.pucp.edu.pe/index.php/themis/article/view/14462>
- Murillo de la Cueva, P. (1999). La construcción del derecho a la autodeterminación informativa. Revista de Estudios Políticos (Nueva Época), (104), 35-60. https://helvia.uco.es/bitstream/handle/10396/2238/REPNE_104_037.pdf?sequence=1&isAllowed=y
- Murillo de la Cueva, P. (2007). Perspectivas del derecho a la autodeterminación informativa. IDP. Revista de Internet, Derecho y Política, (5), 18-32. <https://www.redalyc.org/pdf/788/78812861003.pdf>
- Ordóñez, L. (2017). La protección de datos personales en los estados que conforman la Comunidad Andina: estudio comparado y precisiones para un modelo interamericano de integración. Foro, Revista de Derecho, (27), 83-114. <https://www.redalyc.org/pdf/900/90075911005.pdf>
- Roel, L. A., Chocano, E. J., & Salazar, P. M. (2025). Las nuevas tecnologías y el daño al derecho a la autodeterminación informativa y derechos conexos. La IA como una nueva amenaza para los derechos

fundamentales. Revista Peruana de Derecho Constitucional, (16), 159–191. <https://revista.tc.gob.pe/index.php/revista/article/view/440>

Sosa, A. (2024). Conflictos entre la autodeterminación informativa y la segmentación de perfiles a través de la publicidad programática online en el Perú. Derecho & Sociedad, (63), 285-298. <https://revistas.pucp.edu.pe/index.php/derechoysociedad/article/view/299>

72