Lima, 19 de julio del 2026

INFORME N° 0002-2026-CJDPYNT

A : **Fiorella Maria Rodriguez Chávez**
Directora de la Autoridad Nacional de Datos Personales

De: **Clínica Jurídica de Derechos de las Personas y Nuevas Tecnologías**
Pontificia Universidad Católica del Perú (PUCP)

Asunto: Informe sobre la insuficiencia del consentimiento informado como mecanismo de protección a la autodeterminación informativa en plataformas digitales.

Tenemos el honor de dirigirnos a usted para saludarle muy cordialmente y, a la vez, trasladarle y hacer de su conocimiento el informe sobre la insuficiencia del consentimiento informado como mecanismo de protección a la autodeterminación informativa en plataformas digitales, con el objetivo de poner a su disposición en análisis realizado por la "**Clínica Jurídica de Derechos de las Personas y Nuevas Tecnologías**"[1] y poner a su disposición las conclusiones desarrolladas en el apartado VII del presente documento:

I. ANTECEDENTES

1.1. Contexto digital

En los últimos años, el desarrollo de las tecnologías digitales y las redes sociales ha transformado la forma en que las personas se relacionan e interactúan en internet. Plataformas como TikTok se han convertido en espacios virtuales de uso cotidiano para millones de usuarios; en particular para los jóvenes, por su capacidad de ofrecer contenido altamente personalizado a partir de algoritmos que determinan perfiles en función a los intereses y comportamientos de los usuarios. El funcionamiento de estas se basa en la recopilación constante de datos personales y conductuales. Cada interacción dentro de la aplicación, ya sea videos vistos, tiempo de permanencia, búsquedas, comentarios o "likes", permite construir perfiles digitales detallados mediante algoritmos e inteligencia artificial. A partir de ello, las plataformas desarrollan sistemas de segmentación publicitaria y personalización de contenido orientados a maximizar la atención y permanencia de los usuarios.

En este contexto digital, los datos personales han adquirido un importante valor económico dentro de la denominada economía digital. El capitalismo de vigilancia utiliza la experiencia y comportamiento de las personas como fuente de información para fines comerciales y predictivos (Zuboff, 2020). Esto genera desafíos para la protección del derecho a la autodeterminación informativa, entendido como la facultad de toda persona de controlar el uso y destino de sus datos personales.

[1] Elaborado por las estudiantes: xxx

Frente a ello, el consentimiento informado ha sido tradicionalmente considerado como el principio rector del sistema de protección de datos personales y, a su vez, el principal mecanismo que legitima el tratamiento de datos personales. Sin embargo, en plataformas digitales complejas como TikTok, cuya característica principal consiste en la personalización de contenido a partir de inferencias, surgen cuestionamientos sobre si el usuario comprende el verdadero alcance y consecuencias del tratamiento de su información personal.

1.2. Problema

El principal problema consiste en analizar si el consentimiento informado, pese a constituir el principal mecanismo de legitimación del tratamiento de datos personales regulado por la Ley N.° 29733, es suficiente para garantizar una protección efectiva del derecho a la autodeterminación informativa de los usuarios frente al tratamiento automatizado de datos personales con fines de perfilamiento y segmentación publicitaria en plataformas digitales como TikTok.

Si bien la Ley Nº 29733 (en adelante, LPDP) exige que el consentimiento sea libre, previo, expreso e informado, en la práctica las políticas de privacidad suelen presentarse mediante textos extensos, técnicos y difíciles de comprender. Además, las finalidades del tratamiento se formulan de manera amplia o ambigua, utilizando expresiones como “mejorar la experiencia del usuario” o “personalizar contenido”, sin explicar claramente el verdadero alcance del uso de los datos personales.

Asimismo, los usuarios generalmente deben aceptar todas las condiciones impuestas por la plataforma para poder acceder al servicio, sin contar con una posibilidad real de negociación o elección específica. Esto genera una evidente asimetría informativa entre las plataformas digitales y los usuarios, convirtiendo muchas veces el consentimiento en un acto meramente formal.

Esta problemática se intensifica de forma drástica cuando los usuarios son menores de edad, un grupo demográfico que constituye una porción sustancial de la audiencia activa en plataformas como TikTok. En el marco legal, el art. 1358 del Código Civil establece que los menores con discernimiento tienen capacidad para celebrar actos jurídicos vinculados a las necesidades ordinarias de su vida diaria (como el pago del transporte público o adquisiciones de consumo básico), sin que estos adolezcan de nulidad. No obstante, resulta jurídicamente cuestionable homologar estas transacciones cotidianas con el otorgamiento del consentimiento para el tratamiento masivo y automatizado de datos personales. Este último proceso desencadena repercusiones complejas, transfronterizas y permanentes que escapan a la comprensión del menor e incluso de muchos adultos. Por ello, la aptitud legal para realizar actos de subsistencia diaria no equivale a la capacidad cognitiva necesaria para ponderar los riesgos de la perfilación algorítmica y la segmentación publicitaria, lo que sepulta la eficacia del consentimiento informado en el entorno digital y desprotege su autodeterminación informativa. Sobre ello, el consentimiento informado atraviesa una “crisis funcional” en entornos dominados por el Big Data y la inteligencia artificial, debido a que los usuarios no pueden comprender completamente los usos futuros de su información personal (Cotino, 2020). Esta situación pone en clara evidencia que el consentimiento, por sí solo, no resulta suficiente para asegurar un control efectivo del tratamiento de los datos personales en estas plataformas.

1.3. Objetivo

Analizar la insuficiencia del consentimiento informado en el tratamiento de datos personales con fines de segmentación publicitaria en TikTok y proponer mecanismos que fortalezcan la protección del derecho a la autodeterminación informativa.

1.4. Justificación

El presente informe resulta relevante debido a la creciente uso de plataformas digitales como TikTok, cuyos modelos de negocio se sustentan en la recopilación y tratamiento masivo de datos personales para fines de segmentación publicitaria. Estas prácticas permiten elaborar perfiles de los usuarios a partir de sus comportamientos, preferencias e interacciones, generando cuestionamientos sobre el nivel de control que realmente conservan sobre su información personal.

Desde un análisis jurídico, se busca analizar si el consentimiento informado resulta un mecanismo suficiente para garantizar el derecho a la autodeterminación informativa, entendido como la facultad de toda persona para decidir y controlar los usos de sus datos personales. En espacios digitales caracterizados por su dificultad tecnológica, el perfilamiento algorítmico y la publicidad personalizada, existen dudas respecto de si la aceptación de políticas de privacidad permite una decisión verdaderamente libre, previa e informada.

También posee relevancia práctica ya que permitirá identificar las limitaciones existentes en la aplicación de la LPDP frente a plataformas digitales globales como TikTok, especialmente respecto de la publicidad personalizada, el perfilado algorítmico y la protección de menores de edad.

Por último, se busca aportar propuestas orientadas al fortalecimiento de la protección de datos personales en el Perú, tomando en consideración experiencias comparadas como el Reglamento General de Protección de Datos de la Unión Europea (GDPR), así como nuevas tendencias vinculadas a la responsabilidad proactiva y la transparencia algorítmica.

II. MARCO NORMATIVO

El marco normativo que se fundamenta requiere de un estudio riguroso de los conceptos jurídicos que configuran la problemática de la insuficiencia del consentimiento informado en plataformas digitales como Tik Tok. Desde una perspectiva garantista, estos conceptos no pueden abordarse de manera aislada, sino como parte de un sistema interconectado que revela la tensión entre el reconocimiento formal de derechos y su efectiva realización en los espacios digitales.

2.1. Derecho a la autodeterminación informativa

El derecho a la autodeterminación informativa constituye una garantía fundamental frente al poder público y privado en la sociedad digital, orientada a proteger la libertad y el control de las personas sobre su información personal dentro de la sociedad digital. En el ordenamiento peruano, este derecho encuentra sustento en el artículo 2, inciso 6 de la

Constitución Política del Perú, que reconoce el derecho de toda persona “a que los servicios informáticos, computarizados o no, públicos o privados, no suministren informaciones que afecten la intimidad personal y familiar”.

De igual forma, el Tribunal Constitucional ha sido especialmente relevante en la configuración de este derecho. En la sentencia recaída en el Expediente N.° 1797-2002-HD/TC, el Tribunal precisó que la autodeterminación informativa constituye un derecho fundamental autónomo que otorga a su titular una especie de “poder de control” sobre el registro, uso, almacenamiento, circulación y difusión de sus datos personales. Este control no se limita a la mera autorización inicial, sino que se proyecta durante todo el ciclo de vida de la información personal (Tribunal Constitucional del Perú, Exp. N.º 1797-2002-HD/TC, fundamento jurídico 3).

Asimismo, el máximo intérprete de la Constitución ha diferenciado este derecho del derecho a la intimidad personal o familiar. Mientras que el numeral 7 del art. 2 de la Constitución protege un ámbito de reserva frente a intromisiones externas, el numeral 6 del mismo dispositivo "garantiza la facultad de todo individuo de poder preservar su vida privada controlando el registro, uso y revelación de los datos que le conciernen" (Sosa, 2024). Esta distinción resulta fundamental, pues el derecho a la autodeterminación informativa no se agota en impedir intromisiones ilegítimas, sino que otorga un poder de control activo que permite al titular decidir sobre el destino y uso de su información personal.

Este derecho surge como respuesta frente al creciente e inevitable desarrollo tecnológico y a la capacidad de las plataformas digitales para recopilar, almacenar y procesar grandes cantidades de información personal mediante sistemas automatizados. Así, ya no se trata únicamente de proteger la privacidad en sentido clásico, sino de garantizar que cada individuo conserve el control sobre el flujo, uso y destino de sus datos personales. La doctrina nacional ha precisado que la autodeterminación informativa “no se agota en la mera protección de la esfera íntima del individuo, sino que se proyecta como una libertad positiva que otorga al ciudadano un poder de disposición y control efectivo sobre su identidad digital” (Landa, 2022). De esta manera, el derecho busca impedir que las personas sean reducidas a simples perfiles digitales construidos mediante algoritmos y sistemas de inteligencia artificial.

El reconocimiento del carácter patrimonial de la información personal resulta central para comprender la relevancia de este derecho. Como señala la doctrina, "la información personal no sólo es susceptible del derecho de propiedad, sino también de tener un valor de mercado" (Boza, 2004). Esta afirmación implica que los datos personales se convierten en un bien patrimonial susceptible de actos de uso, disfrute, disposición y reivindicación, lo que otorga a su titular la facultad de decidir quiénes pueden tener acceso a su información privada y con qué finalidades. Este enfoque resulta particularmente relevante en el contexto de la economía digital, donde los datos personales han adquirido un valor comercial significativo.

En aplicaciones como TikTok, este derecho adquiere especial relevancia debido a que el tratamiento de datos no se limita únicamente a la información entregada voluntariamente por el usuario como nombre, edad, ubicación geográfica, profesión o intereses, sino que también aquella información generada diariamente con las interacciones en la plataforma, la cual puede reflejar "los productos que agradan o desagradan (por medio de reacciones), el contenido que se sigue y comparte, preferencias políticas y religiosas, lugares preferidos

para comer o divertirse cada vez que se etiqueta a algún local comercial" (Sosa, 2024). Todo este cúmulo de información es utilizado por las redes sociales para obtener rentas mediante el servicio publicitario que ofrecen, lo que evidencia cómo el modelo de negocio de estas plataformas se sustenta en la explotación de los datos personales de los usuarios.

Así, la autodeterminación informativa funciona como un límite frente al poder de las plataformas digitales y como un mecanismo de protección frente a tratamientos desproporcionados o poco transparentes de información personal. Como sostiene la doctrina, este derecho representa "el derecho a mantener el control sobre las propias informaciones personales" (Rodotà, 2009), especialmente en contextos donde el tratamiento automatizado de datos puede afectar la libertad, dignidad y autonomía de las personas. En entornos digitales complejos como Tik Tok, donde los algoritmos de perfilamiento y segmentación publicitaria operan de manera opaca, el ejercicio efectivo de este derecho se ve seriamente comprometido, pues el usuario difícilmente puede conocer con precisión qué datos son recopilados, qué inferencias se realizan sobre su comportamiento y con qué criterios se construyen los perfiles publicitarios que determinan la publicidad que recibe.

2.2. Protección de datos personales

La protección de datos personales constituye el conjunto de principios, normas y mecanismos jurídicos destinados a garantizar que el tratamiento de información personal se realice respetando los derechos fundamentales de las personas, particularmente su privacidad, dignidad y autodeterminación informativa.

En el Perú, este ámbito se encuentra regulado principalmente por la LPDP, la cual establece obligaciones para todas aquellas entidades públicas o privadas que recopilen, almacenen o utilicen información de personas naturales. Dicha normativa reconoce principios fundamentales como legalidad, consentimiento, finalidad, proporcionalidad, seguridad y transparencia, los cuales buscan limitar el tratamiento arbitrario o excesivo de datos personales. En ese sentido, la protección de datos personales no implica prohibir el tratamiento de información, sino garantizar que este se realice de manera legítima, proporcional y compatible con los derechos de los titulares. Sobre ello, la protección de datos personales debe entenderse como “una disciplina de control de riesgos y asimetrías donde el legislador busca equilibrar la libre circulación de información con la mitigación de los abusos derivados de la recopilación masiva de datos” (Sumar, 2021).

Actualmente, el desarrollo de tecnologías como inteligencia artificial, Big Data y sistemas de perfilado automatizado ha generado nuevos desafíos para la protección de datos personales. Espacios digitales como TikTok realizan tratamientos complejos de información mediante algoritmos capaces de analizar comportamientos, generar perfiles predictivos y dirigir publicidad personalizada a partir de datos conductuales de los usuarios.

En este contexto, la protección de datos personales adquiere una dimensión más amplia, pues ya no solo busca evitar la divulgación indebida de información, sino también limitar prácticas de vigilancia, perfilamiento y manipulación conductual derivadas del tratamiento masivo de datos. Por ello, el Reglamento General de Protección de Datos de la Unión Europea (GDPR) ha reforzado principios como la responsabilidad proactiva (accountability), la transparencia algorítmica y la privacidad desde el diseño (privacy by design), orientados a fortalecer la protección efectiva de los usuarios frente a entornos digitales cada vez más complejos.

2.3. Consentimiento informado

El consentimiento informado constituye uno de los principios rectores y principales mecanismos de legitimación para el tratamiento de datos personales dentro del derecho de protección de datos. En el ordenamiento jurídico peruano, la LPDP establece que el tratamiento de datos personales solo puede efectuarse previo consentimiento informado, expreso e inequívoco del titular. El artículo 18 de la misma norma desarrolla el derecho de información del titular, quien debe ser informado en forma detallada, sencilla, expresa, inequívoca y de manera previa a su recopilación, sobre la finalidad para la que sus datos personales serán tratados.

La finalidad de este principio es garantizar que las personas mantengan el control de su información personal y puedan decidir conscientemente respecto del uso de sus datos. El consentimiento informado se posiciona como piedra angular en la concesión al interesado de un control efectivo sobre sus datos personales. En ese sentido, se encuentra estrechamente vinculado con el derecho a la autodeterminación informativa, ya que busca asegurar que el titular comprenda quién tratará sus datos, con qué finalidad y cuáles serán las consecuencias de dicho tratamiento.

En la práctica, el consentimiento en plataformas como TikTok se otorga de manera global o en bloque, convirtiéndose en una condición necesaria para acceder al servicio. Expresiones como *“if you do not agree with this policy, you should not use the Platform”* evidencian que el usuario no cuenta con una verdadera libertad de decisión, lo que desnaturaliza el carácter libre del consentimiento y lo convierte en un mero requisito formal desprovisto de contenido sustancial.

Esta dinámica resulta especialmente preocupante si se considera que, en el contexto de la sociedad de la información, "el ser humano es y será lo que reflejen sus datos personales o lo que se interprete de los mismos" (Remolina, 2005). Esta afirmación cobra una relevancia particular en plataformas como Tik Tok, donde los algoritmos no solo recopilan información proporcionada voluntariamente por el usuario, sino que también generan inferencias sobre sus preferencias, hábitos de consumo, intereses y patrones de comportamiento, construyendo así una identidad digital sobre la cual el usuario tiene escaso o nulo control. El derecho a la protección de datos personales se concreta precisamente en el derecho de las personas a controlar sus propios datos, por ello es fundamental que el titular de la información conozca la finalidad específica que justifica su uso y el tratamiento destinado a sus datos, ya que al no tener control sobre la información está en riesgo de vulneración del derecho.

Como señala Gallego Fernández, "el enfoque normativo vigente para la protección de datos implica un conjunto de derechos otorgados a sus titulares, por lo tanto, el consentimiento legitima casi cualquier tipo de recolección, uso o divulgación de datos personales" (2015, p. 3). Esta dinámica resulta especialmente problemática en plataformas como TikTok, donde la recolección masiva de datos y la opacidad de los algoritmos impiden que el usuario ejerza un control efectivo sobre su información. En este contexto, "debido al exceso de entidades recolectando y utilizando datos personales, la gente no puede autogestionar o encargarse directamente de su privacidad de manera apropiada" (Gallego Fernández, 2015, p. 3). Esta imposibilidad práctica desnaturaliza la función protectora del consentimiento, convirtiéndo

en un mero requisito formal que legitima tratamientos masivos de datos que el usuario no puede gestionar ni comprender plenamente.

Como se ha evidenciado a lo largo del presente apartado, el consentimiento informado, pese a ser el principal mecanismo de legitimación del tratamiento de datos personales en el ordenamiento jurídico peruano, enfrenta serias limitaciones estructurales en entornos digitales caracterizados por la complejidad tecnológica, la opacidad algorítmica y la asimetría informativa entre plataformas y usuarios. Las exigencias normativas de que el consentimiento sea libre, previo, expreso e informado resultan difícilmente satisfechas en la práctica cuando, como ocurre en TikTok, el acceso al servicio se condiciona a la aceptación global de políticas de privacidad extensas y redactadas en un lenguaje técnico que el usuario promedio no comprende.

2.4. Economía de datos

La economía de datos representa un modelo económico contemporáneo en el cual los datos personales se han convertido en recursos estratégicos y activos de gran valor comercial para las empresas tecnológicas. En ese contexto, plataformas digitales como TikTok basan gran parte de su funcionamiento y rentabilidad en la recopilación, análisis y explotación masiva de información de los usuarios. A diferencia de los modelos tradicionales de consumo, el usuario no paga necesariamente por el servicio mediante dinero, sino a través de la entrega casi permanente de información personal y conductual. Cada reproducción, búsqueda, comentario, “like” o tiempo de permanencia dentro de la plataforma genera datos que son procesados mediante algoritmos e inteligencia artificial para construir perfiles digitales altamente detallados. La economía de datos no se limita únicamente a la información proporcionada conscientemente por el usuario, sino que se sustenta también en un “ecosistema de inferencias”, donde las plataformas pueden deducir intereses, preferencias, hábitos de consumo e incluso características personales a partir del análisis automatizado de datos conductuales.

Al respecto, el término “capitalismo de vigilancia” consiste en utilizar la experiencia humana como fuente de extracción de datos para fines predictivos y comerciales (Zuboff, 2020). En similar sentido, Viktor Mayer-Schönberger y Kenneth Cukier afirman que “*data has become a new economic asset class*” (Mayer-Schönberger & Cukier, 2013), resaltando el valor estratégico que posee actualmente la información personal dentro de la economía digital. Asimismo, la economía de datos contemporánea opera bajo un sistema donde la experiencia interactiva de los usuarios es transformada en “datos de comportamiento predictivo altamente cotizados por el mercado publicitario” (Alvites Mendoza, 2023). Bajo esta lógica, la interacción de los usuarios con las plataformas digitales, ha dejado de ser un simple registro de información, para convertirse en un dato sustancial que las empresas usan para fines comerciales.

En consecuencia, las plataformas digitales desarrollan mecanismos de segmentación publicitaria y perfilado automatizado capaces de influir en la conducta de las personas mediante recomendaciones de contenido y publicidad hiper personalizada. Este modelo genera, además, una evidente asimetría informativa estructural entre las plataformas tecnológicas y los usuarios, ya que las empresas responsables del tratamiento de datos poseen herramientas de análisis, perfilado y algoritmos opacos que superan ampliamente la capacidad de comprensión y supervisión del individuo promedio.En ese contexto, Pasquale

sostiene que los "algoritmos de caja negra pueden moldear el comportamiento humano sin una rendición de cuentas ni una transparencia significativas[2] (2015, p. 3), aludiendo a la falta de mecanismos efectivos que permitan conocer y controlar el funcionamiento de dichos sistemas. Por ello, la economía de datos plantea nuevos desafíos para la protección de derechos fundamentales como la privacidad, la autodeterminación informativa y la transparencia en el tratamiento automatizado de datos personales.

III. FUNCIONAMIENTO DEL MODELO DE NEGOCIO DE LAS REDES SOCIALES: EL CASO DE TIKTOK

3.1. ¿Qué clase de datos recopila Tiktok?

La política de privacidad de TikTok, en su versión actualizada por última vez el 2 de junio de 2025, establece que esta aplicación recopila información de tres maneras

- Información proporcionada por el usuario: Esta información incluye aquella que el usuario proporciona sobre la cuenta (e.g. fecha de nacimiento, nombre de usuario, correo electrónico, etc.); contenido que el usuario crea, sube o comparte en la aplicación y los metadatos asociados; mensajes enviados a través de la aplicación; información de las compras que se realizan en la plataforma; entre otros.
- Información recopilada automáticamente: Esto incluye la información del dispositivo y conexión a la plataforma; información sobre la ubicación del usuario; información de cómo el usuario interactúa con el contenido y la publicidad, duración y frecuencia de las interacciones; características del contenido que consume el usuario; información inferida e intereses del usuario; entre otros.
- Información de otras fuentes: Hace referencia a la información obtenida de otros anunciantes y socios de medición sobre acciones del usuario fuera de la plataforma; información proporcionada por vendedores y proveedores de pago; datos proporcionados a plataformas de terceros y socios.

3.2. ¿Para qué se utilizan los datos recopilados?

Por su parte, la política de privacidad de TikTok también describe cómo y con qué finalidades se utiliza la información recopilada. Entre los principales objetivos se encuentra (1) proporcionar y administrar la plataforma para que el usuario pueda crear, compartir y consumir contenidos, interactuar con otros usuarios y sus contenidos; (2) proporcionar las funciones de compras, de productos, bienes y servicios y para compartir dicha información con vendedores; (3) personalizar y adaptar las funciones y contenidos; y (4) proporcionar servicios de publicidad, incluida la publicación de anuncios (entre otros, anuncios personalizados, siempre que esté permitido).

En primer lugar, la finalidad de proporcionar y administrar la plataforma implica que TikTok realiza actividades necesarias para garantizar el correcto funcionamiento de los servicios ofrecidos por su plataforma. Ello incluye la creación y gestión de cuentas del usuario, la autenticación de la identidad de las personas registradas, la posibilidad de crear, publicar y

[2] The power to include, exclude, and rank is the power to ensure that certain public impressions become permanent, while others remain fleeting." Frank Pasquale, *The Black Box Society: The Secret Algorithms That Control Money and Information* (Harvard University Press, 2015).

compartir contenido, así como la interacción con otros usuarios mediante comentarios, mensajes, reacciones y demás herramientas (TikTok, 2025).

En segundo lugar, TikTok utiliza la información recopilada para proporcionar funciones de compra de productos, bienes y servicios disponibles dentro de la plataforma. Esto permite a los usuarios explorar y adquirir bienes o servicios sin salir de la aplicación. Toda la información de navegación y de productos es procesada por la plataforma y compartida con los vendedores para gestionar y cumplir con los pedidos (TikTok, 2025).

En tercer lugar, la empresa emplea los datos recopilados para personalizar y adaptar las funciones y contenidos que se muestran a cada usuario. Esta finalidad permite que la experiencia de navegación sea diseñada de acuerdo con los intereses, preferencias y comportamientos de cada persona. Para lograr ello, TikTok analiza información relacionada con las búsquedas realizadas, los videos visualizados, el tiempo de permanencia en determinados contenidos, las interacciones efectuadas y otros patrones de uso.(TikTok, 2025). Sobre la base de dicho análisis, la plataforma recomienda contenidos, cuentas, tendencias y funcionalidades que considera relevantes para cada usuario, con el propósito de incrementar su participación e interacción dentro del servicio.

Finalmente, TikTok utiliza la información recopilada para proporcionar servicios publicitarios, incluida la publicación de anuncios personalizados. Esta finalidad supone el análisis de datos relativos a las actividades, intereses y preferencias de los usuarios con el objetivo de mostrar publicidad que resulte más relevante para cada persona. En ese sentido, Tiktok se ha convertido en la red social favorita para promocionar debido al engagement que tiene en sus usuarios (Vicente y Diaz, 2024). En tal sentido, una de las principales finalidades del tratamiento de datos personales realizado por Tiktok es la personalización publicitaria, para lo cual se requiere el perfilado de información de sus usuarios.

3.3. ¿Cómo funcionan los algoritmos en Tiktok?

Los algoritmos son los encargados de procesar la información recopilada de los usuarios y transformarla en recomendaciones personalizadas de contenido (Pauner, 2023). Su papel es fundamental para la experiencia de navegación dentro de la plataforma, pues permiten que cada usuario reciba una selección individualizada de videos en función de sus preferencias y comportamientos de consumo digital.

El sistema de recomendación de TikTok, conocido popularmente como For You, no se encuentra conformado por un único algoritmo, sino por diversos sistemas algorítmicos que analizan continuamente la actividad de los usuarios. Estos sistemas evalúan factores como los videos visualizados, los “me gusta”, los comentarios, las búsquedas realizadas, las cuentas seguidas y, especialmente, el tiempo dedicado a consumir cada tipo de contenido. A partir de esta información, la plataforma identifica patrones de comportamiento y predice qué contenidos tienen mayores probabilidades de captar la atención de cada usuario, ofreciendo recomendaciones altamente personalizadas (Wang, 2020). De esa manera, el sistema de recomendación que realiza de Tiktok se fundamenta en el análisis automatizado de las interacciones de los usuarios con la plataforma.

La eficacia de este sistema se relaciona también con las características del contenido difundido en la plataforma. TikTok se basa principalmente en videos de corta duración,

comúnmente denominados fast content, cuya extensión suele oscilar entre pocos segundos y un minuto. Según Wang (2020), este formato favorece un consumo rápido y continuo de contenidos, permitiendo que el algoritmo obtenga información constante sobre las preferencias de los usuarios y ajuste de manera inmediata las recomendaciones que les presenta.

3.4. La segmentación publicitaria

Tiktok es una de las plataformas preferidas para que las marcas puedan promocionar sus productos, gracias a la gran cantidad de datos recopilados sobre las preferencias, intereses y comportamientos de los usuarios, la plataforma puede ofrecer a las empresas herramientas que le permiten dirigir sus anuncios hacia audiencias específicas. En esa línea, TikTok cuenta con TikTok Ads, su plataforma publicitaria oficial, a través de la cual los anunciantes pueden crear, gestionar y optimizar campañas de marketing digital. Esta herramienta permite segmentar audiencias considerando criterios demográficos, como edad, sexo y ubicación geográfica, así como variables relacionadas con intereses, comportamientos de navegación, interacciones dentro de la aplicación y hábitos de consumo de contenido.

La efectividad de TikTok Ads se encuentra estrechamente vinculada al funcionamiento de los algoritmos de recomendación de la plataforma. En ese sentido la publicidad en TikTok se caracteriza por integrarse de manera natural dentro del flujo de contenido consumido por los usuarios. Cortés y Vizcaíno (2025), sostienen que esta integración favorece una mayor interacción con las marcas, ya que los anuncios suelen presentarse con formatos similares a los videos orgánicos de la plataforma. Entre los formatos más utilizados se encuentran los In-Feed Ads, los TopView Ads, los Branded Hashtag Challenges y los Branded Effects, los cuales buscan fomentar la participación activa de los usuarios y aumentar la visibilidad de las marcas

IV. INSUFICIENCIA DEL CONSENTIMIENTO INFORMADO

4.1. Problemas prácticos

La insuficiencia del consentimiento informado se manifiesta en plataformas digitales como TikTok. Aunque formalmente los usuarios aceptan políticas de privacidad y términos de uso antes de utilizar la aplicación, ello no implica necesariamente que comprendan el alcance real del tratamiento de sus datos personales. En la práctica, el consentimiento suele obtenerse mediante mecanismos estandarizados, como casillas de aceptación o botones de "Aceptar", sin que exista un proceso efectivo que garantice la comprensión del contenido por parte del usuario. Así, el cumplimiento formal del requisito legal no siempre se traduce en una decisión libre e informada.

A ello se suma el fenómeno conocido como “fatiga del consentimiento”, mediante el cual los usuarios se enfrentan constantemente a solicitudes de autorización, lo que genera comportamientos automatizados de aceptación sin una lectura previa o análisis real de las condiciones propuestas. Como consecuencia, el consentimiento pierde su función informativa y se convierte en un trámite necesario para acceder al servicio (Lilla, 2023, como se cita en Abrusio, 2024). Dicho fenómeno se intensifica en aplicaciones de uso cotidiano como TikTok, donde las actualizaciones frecuentes de las políticas de privacidad y

de los términos del servicio incentivan que los usuarios acepten sucesivas modificaciones sin conocer qué aspectos del tratamiento de datos han cambiado.

Otro problema relevante se encuentra en la utilización de algoritmos de perfilamiento y segmentación publicitaria. TikTok recopila información relativa a interacciones, hábitos de navegación, preferencias de consumo, ubicación, tiempo de visualización y comportamiento digital del usuario. A partir de dichos datos, la plataforma construye perfiles predictivos destinados a personalizar contenidos y publicidad. No obstante, el usuario difícilmente puede conocer el funcionamiento interno de estos sistemas ni prever las inferencias que serán obtenidas a partir de su información personal. Por tanto, el consentimiento inicialmente otorgado resulta insuficiente para abarcar tratamientos futuros que ni siquiera la propia plataforma puede describir de forma específica al momento de la recolección de los datos, debido a que los algoritmos generan nuevas inferencias y categorías de información conforme interactúan con el comportamiento del usuario.

Ello resulta preocupante cuando se trata de menores de edad, quienes constituyen una parte significativa de la base de usuarios de la plataforma. En estos casos, surgen cuestionamientos sobre la validez y suficiencia del consentimiento otorgado para el tratamiento de sus datos personales, ya que los menores pueden no comprender plenamente el alcance de la recopilación de información, el perfilamiento automatizado y sus posibles consecuencias. Asimismo, la obtención del consentimiento de los representantes legales no siempre es verificable de manera efectiva, lo que incrementa los riesgos de vulneración del derecho a la protección de datos personales y del principio del interés superior del niño. Incluso desde el derecho civil peruano, si bien el artículo 1358 del Código Civil permite que los menores con discernimiento celebren actos vinculados con las necesidades ordinarias de su vida cotidiana, dicha habilitación difícilmente puede extenderse al consentimiento para tratamientos complejos de datos personales, cuyos efectos jurídicos y tecnológicos excede aquello que razonablemente puede comprender un menor de edad.

Desde el ordenamiento, la Constitución reconoce el derecho fundamental a la protección de los datos personales en su art. 2, inciso 6, indicando que las plataformas y servicios digitales no deben afectar la intimidad de las personas, mientras que la LPDP, en su artículo 2, dentro de las características del consentimiento, se indica que este debe ser “libre, previo, expreso e informado”. Asimismo, la normativa reconoce derechos de acceso, rectificación, cancelación y oposición respecto de los datos personales tratados por terceros. Sin embargo, la aplicación efectiva de estas garantías enfrenta importantes obstáculos en el entorno digital. En la práctica, los usuarios suelen desconocer qué datos recopila la plataforma, con qué finalidades son utilizados y cuáles son los procedimientos para ejercer sus derechos. A ello se añade que las finalidades del tratamiento suelen formularse de manera amplia, utilizando expresiones como "desarrollar nuevos servicios" o "personalizar contenido", sin precisar qué operaciones concretas se realizarán sobre los datos personales ni cuáles serán sus destinatarios, lo que limita significativamente la posibilidad de otorgar un consentimiento verdaderamente informado

Si bien existen mecanismos de tutela administrativa ante la Autoridad Nacional de Protección de Datos Personales y mecanismos constitucionales como el proceso de hábeas data, estos remedios suelen activarse únicamente cuando el usuario identifica una afectación concreta a sus derechos. El problema radica en que los tratamientos algorítmicos

y las técnicas de perfilamiento actúan de forma poco clara, lo cual no facilita que los usuarios identifiquen si sus datos están siendo vulnerados. Además de ello, para poder realizar acciones legales en contra de las plataformas, se requiere de conocimientos jurídicos e informáticos, con los que no cuentan la media de los usuarios.

En consecuencia, aunque el ordenamiento jurídico peruano reconoce mecanismos de protección frente al tratamiento indebido de datos personales, estos resultan limitados para afrontar los desafíos que plantean las plataformas digitales basadas en inteligencia artificial y sistemas de perfilamiento masivo. La asimetría informativa entre la plataforma y los usuarios, la complejidad tecnológica de los algoritmos y el escaso conocimiento ciudadano sobre los mecanismos de tutela disponibles reducen significativamente la eficacia práctica del consentimiento informado como instrumento de protección de la privacidad. Por ello, la discusión jurídica contemporánea se orienta hacia modelos regulatorios que complementen el consentimiento con obligaciones reforzadas de transparencia, responsabilidad proactiva, evaluaciones de impacto y restricciones específicas al tratamiento automatizado de datos personales, especialmente cuando involucran perfiles de menores de edad o decisiones basadas en inteligencia artificial

4.2. Asimetría informativa

En los entornos digitales actuales existe una marcada brecha entre la teoría y la práctica. El modelo tradicional de consentimiento parte de una lógica individualista que presume que el usuario posee la capacidad de comprender políticas de privacidad complejas y ejercer un control efectivo sobre su información personal. No obstante, las plataformas digitales suelen presentar términos y condiciones extensos, redactados en lenguaje técnico y con finalidades ambiguas, dificultando una comprensión real del alcance del tratamiento.

En plataformas como TikTok, el consentimiento suele otorgarse de manera global o “en bloque”, convirtiéndose en una condición necesaria para acceder al servicio. Expresiones como “if you do not agree with this policy, you should not use the Platform” evidencian que el usuario no cuenta con una verdadera libertad de decisión, lo que desnaturaliza el carácter libre del consentimiento y lo convierte muchas veces en un acto meramente formal. Asimismo, el uso de expresiones amplias como “improve user experience” o “personalize content” impide que el titular conozca de manera concreta el verdadero alcance del tratamiento de sus datos personales. En consecuencia, el consentimiento deja de representar una decisión plenamente consciente e informada.

El consentimiento informado “requiere que el titular comprenda a cabalidad las consecuencias legales y prácticas de proporcionar su información, lo cual obliga al responsable del tratamiento a comunicar las finalidades bajo estándares de máxima claridad y transparencia” (Zegarra, 2019). El consentimiento informado atraviesa una “crisis funcional” en escenarios dominados por el Big Data y la inteligencia artificial, debido a que el usuario no puede prever los usos futuros de su información ni comprender completamente el funcionamiento de los sistemas algorítmicos (Cotino, 2020).

En consecuencia, el modelo tradicional basado únicamente en el consentimiento individual evidencia importantes limitaciones frente a plataformas digitales que utilizan algoritmos, perfilado automatizado y sistemas masivos de recopilación de información personal.

V. ANÁLISIS JURÍDICO

5.1. Perú: Ley N° 29733 y principios aplicables

La protección de los datos personales constituye un fundamento constitucional en el derecho a la autodeterminación informativa reconocido en el art. 2, inciso 6 de la Constitución. Este derecho ha sido desarrollado por el Tribunal Constitucional como la facultad que posee toda persona para controlar la recopilación, almacenamiento, uso, tratamiento y difusión de su información personal, constituyendo un verdadero poder de control sobre el ciclo de vida de sus datos.

En desarrollo de este mandato, la LPDP, y su Reglamento establecen una serie de principios que deben regir ante cualquier tratamiento de datos personales, especialmente en entornos digitales caracterizados por el uso de algoritmos de perfilamiento masivo, como ocurre en plataformas como TikTok.

Uno de los principios centrales es el **principio de consentimiento**, regulado en el art. 2 de la Ley, según el cual el consentimiento debe ser “libre, previo, expreso, informado e inequívoco” pero en las plataformas digitales contemporáneas este requisito enfrenta importantes desafíos. Las políticas de privacidad suelen ser extensas, técnicas y redactadas mediante conceptos ambiguos como “mejorar la experiencia del usuario” o “personalizar contenido”, sin explicar de forma comprensible el alcance real del tratamiento de datos. Asimismo, la práctica conocida como “take-it-or-leave-it” (tómalo o déjalo), mediante la cual el usuario debe aceptar integralmente las condiciones para acceder al servicio, cuestiona seriamente la libertad real de elección y transforma el consentimiento en una mera formalidad contractual.

De igual manera, el **principio de finalidad**, recogido en el art. 6, exige que los datos personales sean recopilados para una finalidad determinada, explícita y legítima pero en aplicaciones como TikTok se observa una difuminación entre la finalidad principal del servicio y finalidades secundarias vinculadas al perfilamiento conductual, la personalización extrema y la publicidad dirigida. Esta acumulación de propósitos dificulta que el usuario identifique con claridad para qué se utilizan realmente sus datos personales.

Por su parte, el **principio de proporcionalidad**, previsto en el art. 7, exige que el tratamiento sea adecuado, relevante y no excesivo respecto de la finalidad perseguida. Desde esta perspectiva, resulta discutible que la recopilación automatizada de metadatos, patrones de navegación, tiempos de permanencia, interacciones y preferencias inferidas sea estrictamente necesaria para el funcionamiento esencial de una red social orientada al entretenimiento. De esa forma, el condicionamiento del acceso al servicio a la aceptación de mecanismos de perfilamiento intensivo podría considerarse desproporcionado respecto de la finalidad principal del servicio También, existe una marcada **asimetría informativa** entre la plataforma y el usuario. Mientras TikTok posee un conocimiento detallado sobre los criterios utilizados por su algoritmo de recomendación, los usuarios carecen de información suficiente para comprender cómo se construyen sus perfiles digitales, qué inferencias se generan sobre su comportamiento y cómo estas determinan los contenidos y anuncios que reciben. Esta situación genera una posición de indefensión que limita la eficacia práctica de los mecanismos de tutela reconocidos por la Ley, tales como los derechos ARCO, el procedimiento administrativo ante la Autoridad Nacional de Protección de Datos Personales y el proceso constitucional de hábeas data.

Así, el uso de algoritmos de configuración desconocida, cuyos criterios de funcionamiento no son transparentes ni fácilmente auditables, plantea importantes desafíos para la protección efectiva de los derechos fundamentales de los usuarios y evidencia una posible crisis funcional del consentimiento informado en los entornos digitales contemporáneos.

5.2. Derecho comparado: GDPR y nuevas tendencias regulatorias

El principal referente internacional en materia de protección de datos es el Reglamento General de Protección de Datos de la Unión Europea, considerado actualmente el estándar más avanzado en la materia. Este instrumento normativo influyó significativamente en las reformas regulatorias adoptadas en distintas jurisdicciones y ofrece herramientas especialmente útiles para abordar los desafíos derivados de la inteligencia artificial y el perfilamiento automatizado.

Entre sus aportes destaca el **principio de responsabilidad proactiva**, en su artículo 5, según el cual las organizaciones no solo deben cumplir las obligaciones legales en materia de protección de datos, sino también demostrar activamente dicho cumplimiento mediante políticas internas, auditorías, registros y mecanismos de supervisión permanente. Asimismo, el GDPR incorpora, implícitamente, en su artículo 25, el **principio de privacidad** desde el diseño y por defecto, que exige integrar medidas de protección de datos desde las etapas iniciales de diseño de productos, servicios y sistemas tecnológicos, minimizando riesgos antes de que estos se materialicen.

Una de las herramientas más relevantes es la Evaluación de Impacto relativa a la Protección de Datos, en el art. 35 del Reglamento. Esta evaluación es obligatoria cuando un tratamiento de datos pueda generar altos riesgos para los derechos y libertades de las personas, especialmente en casos de elaboración de perfiles, toma automatizada de decisiones o monitoreo sistemático de comportamientos. Dado que el algoritmo “Para ti” de TikTok realiza perfilamiento predictivo masivo y procesamiento automatizado de grandes volúmenes de información personal, este tipo de mecanismos constituye un referente relevante para futuras actuaciones regulatorias en el Perú. En esa línea, la reciente aprobación del Decreto Supremo N° 016-2024-JUS, que actualiza el Reglamento de la LPDP, ha incorporado expresamente conceptos relacionados con la elaboración de perfiles y las evaluaciones de impacto en protección de datos. Esto permite sostener que la ANPD cuenta actualmente con una base normativa más robusta para supervisar tratamientos automatizados de alto riesgo, aunque todavía subsisten debates respecto al alcance exacto de dichas facultades frente a sistemas complejos de inteligencia artificial.

Específicamente, una de las cuestiones jurídicas más relevantes consiste en determinar si la Autoridad Nacional de Protección de Datos Personales posee actualmente facultades suficientes para exigir evaluaciones de impacto en tratamientos algorítmicos complejos como el sistema “Para ti” de TikTok o si, por el contrario, sería necesaria una reforma legislativa expresa. Si bien la LPDP no reguló originalmente esta figura de manera específica, la incorporación de las evaluaciones de impacto y de la elaboración de perfiles mediante el Decreto Supremo N.° 016-2024-JUS permite sostener que existe una base normativa que habilitaría una interpretación extensiva de las facultades de supervisión de la ANPD.

Desde este análisis, el principio de proporcionalidad y las potestades de fiscalización de la autoridad podrían justificar la exigencia de mecanismos preventivos de evaluación para tratamientos automatizados de alto riesgo pero otra posición sostiene que una obligación de esta naturaleza requeriría una regulación legal expresa que delimite claramente su alcance, contenido y consecuencias jurídicas. La discusión resulta especialmente relevante porque determina si medidas como las auditorías algorítmicas y las evaluaciones de impacto pueden implementarse inmediatamente mediante actuación administrativa o si dependen de una futura reforma normativa. Para efectos del presente informe, se considera que el marco regulatorio vigente, particularmente tras la entrada en vigor del Decreto Supremo N.° 016-2024-JUS, ofrece fundamentos suficientes para que la ANPD desarrolle lineamientos técnicos y exija evaluaciones de impacto en determinados sistemas de perfilamiento algorítmico de alto riesgo, sin perjuicio de que una reforma legislativa posterior pueda otorgar mayor seguridad jurídica y precisión regulatoria.

Otra tendencia importante es el fortalecimiento del consentimiento granular, desarrollado por las directrices europeas del antiguo Grupo de Trabajo del Art. 29 y posteriormente por el Comité Europeo de Protección de Datos. Este enfoque exige que los usuarios puedan consentir separadamente distintas finalidades del tratamiento de datos evitando mecanismos de aceptación global que desnaturalizan la libertad de elección. También, el Dictamen 8/2024 del EDPB ha abordado los denominados modelos de “Consentimiento o Pago”, cuestionando la validez de obligar a los usuarios a elegir entre aceptar el perfil publicitario o pagar una tarifa para acceder al servicio. Según dicho organismo, las plataformas de gran escala deberían ofrecer alternativas equivalentes que permitan el acceso al servicio sin requerir necesariamente la aceptación de publicidad comportamental.

Por último, una de las tendencias regulatorias más importantes es la promoción de la transparencia algorítmica y del denominado derecho a una explicación significativa. Bajo esta perspectiva, no basta con publicar políticas generales de privacidad; también resulta necesario que los usuarios comprendan de manera clara por qué reciben determinados contenidos o anuncios, qué categorías o inferencias se han construido sobre ellos y cómo estas influyen en las decisiones automatizadas adoptadas por la plataforma.

Por ello, la experiencia europea evidencia una evolución desde un modelo centrado exclusivamente en el consentimiento hacia uno basado en la gestión preventiva de riesgos, la responsabilidad empresarial y la supervisión activa de sistemas automatizados. Estas tendencias ofrecen criterios valiosos para fortalecer la protección de los usuarios peruanos frente a prácticas de perfilamiento algorítmico intensivo desarrolladas por plataformas digitales como TikTok.

Elementos	**Perú (Reglamento y Ley No. 2973)**	**Unión Europea (GDPR)**
Consentimiento	“libre, previo, expreso, informado e inequívoco” (art 2)	libre, específico, informado y con granularidad.
Finalidad	Determinada, explícita y legítima.	Determinada, explícita y legítima. Adicionalmente, contiene un fuerte control

		respecto a la reutilización de datos
Proporcionalidad	Brindar datos adecuados y no excesivos	Principio de minimización de datos
Responsabilidad	Obligaciones para el titular que recepciona los datos	Principio de responsabilidad proactiva
Privacidad	Insertada en el Reglamento	Regulado en el artículo 25 del GDPR
Evaluación de impacto	Referenciado en el D.S. No. 016-2024-JUS	Obligatorio para tratamientos de alto riesgo (art 35 del GDPR)
Creación de perfiles	Referenciado en el artículo 6 del reglamento	Amplio desarrollo, señalado en el artículo 35 del GDPR
Supervisión	ANPD	Autoridades nacionales, normas internas y el EDPB

VI. PROPUESTA DE MECANISMO DE PROTECCIÓN

El consentimiento informado como mecanismo de legitimación del tratamiento de datos personales ha evidenciado una crisis estructural en plataformas como TikTok. Esta insuficiencia no responde a una única causa, sino a tres deficiencias concurrentes: la ausencia de una alternativa real que permita al usuario acceder al servicio sin someterse al perfilamiento publicitario, la opacidad radical sobre el destino y uso concreto de los datos personales, y la falta de granularidad en el consentimiento que se presenta como un acto único e indivisible.

Frente a ello, proponemos, ante la ANPD, un mecanismo de protección articulado en tres pilares interdependientes que operan en cadena: la libertad de elección mediante el desacoplamiento del servicio esencial; el conocimiento real a través de la transparencia algorítmica objetiva; y el control efectivo mediante la granularidad del consentimiento. Estos tres elementos no son alternativos, sino complementarios y mutuamente reforzantes, pues la ausencia de cualquiera de ellos perpetúa aquella situación de asimetría informativa y poder que caracteriza la relación entre los usuarios y las plataformas digitales

6.1. Desacoplamiento del servicio esencial y libertad real de elección

Tiktok condiciona actualmente el acceso a su servicio a la aceptación íntegra de sus políticas de privacidad y términos y condiciones de uso, lo cual resulta contrario a la exigencia de que el tratamiento de datos deba ser necesario para llevar a cabo servicio esencial contratado por el usuario. Según dichas políticas, entre otros fines, Tiktok realiza el tratamiento de datos de los usuarios con fines de segmentación publicitaria mediante el perfilamiento conductual y elaboración de interferencias predictivas. La política de privacidad de Tiktok incluye - de forma general - que la base jurídica para el tratamiento de datos se sustenta en la “necesidad contractual” - orientado a la administración,

personalización de funciones y contenido de la plataforma -, los “intereses legítimos” de Tiktok, los usuarios o un tercero; y en el consentimiento otorgado por el usuario.

Estas finalidades son contempladas debido a que la normativa europea en materia de protección de datos personales exige que el tratamiento se sustente en una base jurídica, lo cual incluye, entre otros, el consentimiento del titular; cuando este sea necesario para la ejecución del contrato; y cuando sea necesario para satisfacer intereses legítimos del responsable del tratamiento. No obstante, si bien Tiktok justifica, en gran medida, el tratamiento de datos de los usuarios en necesidades contractuales, lo cierto es que el usuario no puede utilizar la plataforma si rechaza dichas finalidades. La dinámica antes descrita - conocida en la doctrina como “tómalo o déjalo” (*take it or leave it)* - constituye una distorsión del consentimiento por falta de libertad real, pues el titular se ve forzado a aceptar tratamientos no esenciales para poder acceder a un servicio que, en la práctica, se ha vuelto relevante para su participación en la vida social, cultural e incluso profesional.

Dicha situación evidencia una profunda asimetría informativa entre la plataforma y el usuario que va más allá de la asimetría inherente a los contratos por adhesión. La doctrina peruana en materia de derecho del consumidor ha señalado que los proveedores cuentan con mayor información sobre sus procesos productivos que los consumidores, lo que justifica la intervención del Estado para nivelar la relación entre las partes (Fuentes & Sánchez, 2017). Esta misma lógica opera con igual o mayor intensidad en las plataformas digitales: TikTok posee un conocimiento exhaustivo sobre el funcionamiento de sus algoritmos y el destino de los datos personales, mientras que el usuario carece de información si quiera mínima para tomar una decisión verdaderamente informada. El desacoplamiento del servicio esencial propuesto constituye, precisamente, un correctivo estructural a esta asimetría.

El Dictamen 8/2024 del Comité Europeo de Protección de Datos (EDPB), adoptado el 17 de abril de 2024, sobre los modelos de “consentimiento o pago” (*consent or pay*) en el contexto de la publicidad conductual, establece criterios de suma relevancia para el problema identificado. Este dictamen, emitido a solicitud de las autoridades de protección de datos de Países Bajos, Noruega y Alemania, analiza específicamente aquellos modelos de negocio en los cuales se ofrece al usuario la posibilidad de elegir entre consentir el tratamiento de sus datos personales con fines de publicidad basada en el comportamiento o pagar una cuota para acceder al servicio sin dicho tratamiento.

El EDPB señala que, en la mayoría de los casos, las grandes plataformas en línea no podrán cumplir con los requisitos para un consentimiento válido si confrontan a los usuarios únicamente con una elección binaria entre consentir al tratamiento de datos para publicidad conductual o pagar una tarifa (EDPB, 2024). La oferta de una alternativa exclusivamente de pago no debe constituir la forma predeterminada de actuación para los responsables del tratamiento.

En este sentido, el Dictamen introduce el concepto de “alternativa equivalente” (*equivalent alternative*), definido como una versión del servicio ofrecida por el mismo responsable que no comprende el consentir al tratamiento de datos personales con fines de publicidad comportamental (EDPB, 2024). Esta alternativa debe cumplir con dos características fundamentales. En primer lugar, debe diferir solo en aquello estrictamente necesario como consecuencia de que el responsable no puede tratar los datos personales con fines de publicidad comportamental, pudiendo considerarse, en principio, equivalente. En segundo lugar, debe ser preferentemente gratuita, pues el EDPB establece que, al desarrollar la

alternativa, las plataformas deben considerar la posibilidad de ofrecer una “alternativa equivalente” que no implique el pago de una tarifa. En caso opten por cobrar dicha tarifa, deben considerar también ofrecer otra alternativa gratuita que incluya una forma de publicidad que requiera el tratamiento de una menor cantidad de datos personales o de ninguno.

Adicionalmente, el EDPB advierte que existe un perjuicio cuando los interesados que no prestan su consentimiento se enfrentan a la exclusión del servicio, especialmente cuando este tiene un papel destacado o es decisivo para la participación en la vida social o el acceso a redes profesionales, más aún en presencia de efectos de dependencia o de red (EDPB, 2024). Como consecuencia de ello, es probable que se produzca un perjuicio cuando las grandes plataformas en líneas utilizan un modelo de “consentimiento o pago” para obtener el consentimiento para el tratamiento. Finalmente, el Dictamen recuerda un principio de singular importancia: los datos personales no pueden considerarse una mercancía comercializable. En tal sentido, los responsables del tratamiento deben evitar que el derecho fundamental a la protección de datos se transforme en una cualidad por la que los interesados deban pagar para disfrutarla.

En consideración a lo anterior, consideramos de suma relevancia que la Autoridad Nacional de Protección de Datos Personales, en ejercicio de sus facultades de supervisión y de interpretación, emita una opinión técnica vinculante, lineamiento o una directriz interpretativa que establezca el principio de servicio esencial sin perfilamiento. Dicho documento podrá desarrollar el alcance del principio, las disposiciones normativas vigentes en las cuales tenga sustento y la aplicación práctica que podría darse en casos concretos. Así, en virtud al principio de servicio esencial sin perfilamiento, ninguna plataforma digital cuyo responsable de tratamiento de datos sea residente peruano o, siendo extranjero, que ofrezca servicio a usuarios residentes en Perú, podrá condicionar el acceso a sus funcionalidades esenciales a la aceptación del tratamiento de datos personales con fines de segmentación publicitaria.

En aplicación de este principio, TikTok debería ofrecer a los usuarios peruanos una versión del servicio que garantice funcionalidades plenas - esto es, visualización de vídeos, interacción mediante likes, comentarios y compartidos, seguimiento de cuenta y mensajería básica - con un modelo de publicidad contextual basada en el contenido del video que se está visualizando o publicidad no personalizada que no emplee el historial de navegación ni inferencias generadas con los datos de los usuarios. Esta versión debe ser gratuita, sin necesidad de suscripción de pago, y sin degradación artificial de la experiencia de usuario. Es decir, sin tiempos de espera, restricciones de contenido o limitaciones funcionales respecto de la versión con publicidad comportamental.

El desacoplamiento propuesto encuentra sustento en el principio de consentimiento libre contemplado en el art. 5 de la LPDP, el cual exige que el consentimiento sea “libre, previo, expreso e informado”. Asimismo, se alinea con el principio de finalidad y proporcionalidad regulado en los artículos 6 y 7 de la misma ley, en virtud de los cuales el tratamiento de datos personales debe ser “adecuado, relevante y no excesivo” en relación con la finalidad para la cual se recogieron. La segmentación publicitaria no constituye una finalidad necesaria para el funcionamiento esencial de una red social como Tik Tok, por lo que resulta desproporcionado condicionar el acceso al servicio a su aceptación incondicionada.

6.2. Derecho a la explicación objetiva del tratamiento algorítmico

A la fecha de elaboración de este informe, Tiktok informa a través de su política de privacidad que utiliza los datos personales de sus usuarios para personalizar el contenido y mostrar publicidad relevante. No obstante, dicha información es presentada de manera general y poco clara. En ese sentido, si bien el usuario sabe que su información está siendo utilizada para fines publicitarios, desconoce cómo se aplicó el tratamiento de sus datos en su caso en particular. En específico, el usuario desconoce qué datos específicos fueron considerados, qué inferencias se realizaron sobre la información proporcionada a la plataforma y cuáles fueron los criterios utilizados por Tik Tok para determinar la presentación de un anuncio en concreto.

Por lo tanto, identificamos que en el caso de Tik Tok la existencia real de consentimiento se ve afectada por la información que precede al otorgamiento del mismo. Tal como sostiene Nissenbaum, la protección de la privacidad requiere que las personas comprendan el contexto y las consecuencias del flujo de información que las involucra, lo cual no se cumple en el caso materia de análisis. En caso no exista una comprensión acerca de la información respecto de la cual el usuario otorgue su consentimiento, la capacidad de control sobre los datos personales se vuelve meramente ilusoria (2020, pp. 12).

Frente a este contexto, se propone que la Autoridad Nacional de Protección de Datos Personales emita lineamientos interpretativos que desarrollen el principio de transparencia regulado en la LPDP en el contexto de la segmentación publicitaria, estableciendo que el mismo no se satisface únicamente con la publicación de políticas de privacidad generales sino que exige mecanismos que permitan al usuario conocer de manera individualizada los efectos del tratamiento de datos sobre su perfil.

En ese sentido se debería instar a que las plataformas digitales cuyo responsable de tratamiento de datos sea residente peruano o, siendo extranjero, que ofrezca servicio a usuarios residentes en Perú (tales como Tik Tok), incluyan información como la que se indica a continuación:

- Qué categorías de datos personales fueron utilizadas para la segmentación publicitaria.
- Qué intereses, preferencias o características fueron inferidos sobre el usuario.
- Qué criterios determinaron su inclusión dentro de un determinado grupo publicitario.
- Qué anunciantes o categorías de anunciantes utilizaron dichos criterios para dirigir la publicidad.

A manera de ilustración, para poder lograr dichos objetivos debería acompañarse cada anuncio con una opción de “¿por qué este anuncio es para mi?” a través del cual el usuario acceda a una explicación individualizada sobre los factores que determinaron la visualización de dicha publicidad. Esta explicación debería incluir, como mínimo, las categorías de datos personales utilizadas, las inferencias realizadas por la plataforma, el segmento publicitario al que fue incorporado el usuario y la relación existente entre dichos elementos y el anuncio mostrado.

Asimismo, la explicación proporcionada no debería limitarse a una descripción genérica del funcionamiento de la publicidad personalizada, sino que tendría que referirse específicamente al caso del usuario. En otras palabras, no bastaría con indicar que la plataforma utiliza datos de navegación o interacción, sino que debería precisarse cuáles de esos datos fueron efectivamente considerados para la segmentación realizada. De esta

manera, el usuario podría comprender de forma concreta cómo la plataforma construye perfiles publicitarios a partir de su actividad digital.

La implementación del mecanismo antes descrito permitiría reducir la asimetría informativa existente entre la plataforma y el usuario. Como sostiene Piñar (2005), la transparencia constituye uno de los pilares esenciales de la protección de datos personales, en tanto permite que los individuos conozcan y controlen el uso que se realiza de su información. En efecto, la autodeterminación informativa presupone que el titular de los datos pueda comprender las consecuencias derivadas del tratamiento de estos, pues de lo contrario cualquier consentimiento otorgado pierde eficacia como manifestación auténtica de voluntad. Adicionalmente, la explicación debería estar acompañada de mecanismos de acción inmediata que permitan al usuario modificar o revocar las categorías de segmentación asignadas. Así, junto con la información sobre los intereses inferidos, TikTok debería ofrecer la posibilidad de corregirlos, eliminarlos o impedir que continúen siendo utilizados para fines publicitarios. Ello transformaría la transparencia en una herramienta efectiva de control y no en una mera obligación formal de información.

La presente propuesta encuentra sustento tanto en experiencias desarrolladas en el derecho comparado como en mecanismos de transparencia ya implementados por algunas plataformas digitales. En primer lugar, un antecedente relevante se encuentra en la Unión Europea a través de la Ley de Servicios Digitales (Digital Services Act – DSA). En particular, mediante su art. 39 establece que las plataformas en línea de muy gran tamaño que difundan publicidad deben poner a disposición del público un repositorio de anuncios que contenga información relativa al contenido del anuncio, la identidad de la persona natural o jurídica que financió su difusión, así como los principales parámetros utilizados para determinar los grupos de destinatarios a los que estuvo dirigido.

No obstante, el mecanismo previsto por el DSA presenta una limitación desde la perspectiva de la experiencia del usuario, pues la información se encuentra alojada en un repositorio independiente al que se debe acceder de manera posterior para localizar el anuncio de su interés y conocer los datos relacionados con su difusión. En consecuencia, si bien dicho modelo constituye un avance significativo en materia de transparencia publicitaria, el acceso a la información continúa dependiendo de una serie de actuaciones adicionales por parte del usuario. En atención a ello, la propuesta formulada en el presente informe implica un mecanismo de transparencia más accesible e inmediato, consistente en incorporar, junto a cada anuncio publicitario mostrado en TikTok, una opción que permita al usuario conocer directamente los elementos que justificaron su segmentación.

En adición a lo anterior, la viabilidad operativa de esta propuesta encuentra respaldo en herramientas ya implementadas por otras plataformas digitales. Un ejemplo de ello es la sección de “por qué veo este anuncio” desarrollado por Google para YouTube cuando este muestra una publicidad. A través de esta funcionalidad, dando un click en la parte derecha baja del video, los usuarios pueden conocer información básica sobre el anunciante. Esta sección incluye el nombre de la empresa y la información que se ha utilizado para mostrar el anuncio, en el cual se señala sólo de forma general dos opciones: la hora y la ubicación geográfica, sin explicar más.

En efecto, esta herramienta no permite identificar de manera específica cuáles fueron los datos personales efectivamente utilizados, qué inferencias elaboró la plataforma respecto del usuario, cuáles fueron los criterios concretos empleados para su incorporación en un determinado segmento publicitario ni la forma en que dichos elementos incidieron en la decisión de mostrar un anuncio específico. Por ello, la presente propuesta plantea fortalecer este tipo de mecanismos mediante la incorporación de explicaciones individualizadas, claras y suficientemente detalladas que permitan al usuario comprender de manera efectiva cómo fue tratado su perfil para efectos de la publicidad personalizada.

En ese sentido, la adopción de estos mecanismos demuestra que las obligaciones de transparencia publicitaria son técnica y jurídicamente viables. Tanto el repositorio de anuncios previsto por la Ley de Servicios Digitales de la Unión Europea, como la herramienta de “por qué veo este anuncio” de Google, representan avances relevantes en la búsqueda de una mayor rendición de cuentas de las plataformas digitales y de un mayor control por parte de los usuarios sobre la publicidad personalizada.

Por lo tanto, desde una perspectiva jurídica, esta propuesta encuentra sustento en el principio de transparencia que inspira la LPDP, así como en el contenido constitucional del derecho a la autodeterminación informativa reconocido por el Tribunal Constitucional peruano y en el artículo 2, inciso 6 de la Constitución. Si el titular tiene derecho a conocer, controlar y decidir sobre el tratamiento de sus datos personales, resulta razonable exigir que las plataformas digitales proporcionen explicaciones comprensibles sobre las decisiones algorítmicas que afectan la publicidad que recibe. En consecuencia, el derecho a la explicación objetiva del tratamiento algorítmico se configura como un mecanismo complementario al consentimiento informado, orientado a fortalecer el control efectivo del usuario sobre sus datos personales en entornos digitales complejos como Tik Tok.

6.3. Granularidad del consentimiento y separación de finalidades

Otro mecanismo de protección consiste en garantizar que el consentimiento del usuario sea otorgado de manera granular y diferenciada según cada finalidad específica del tratamiento de datos personales. Esto responde a una de las principales deficiencias identificadas en el modelo actual de TikTok: la obtención de un consentimiento único, global e indivisible para múltiples tratamientos de datos con finalidades heterogéneas.

A la fecha de elaboración de este informe, las políticas de privacidad de las plataformas digitales suelen agrupar en una sola aceptación diversas actividades de tratamiento, tales como la creación y administración de la cuenta, la personalización del contenido, la segmentación publicitaria, la elaboración de perfiles conductuales, el intercambio de información con socios comerciales y el desarrollo de nuevos productos o servicios. Como consecuencia de lo anterior, el usuario no puede decidir de manera autónoma respecto de cada una de estas finalidades, sino que se ve obligado a aceptarlas en bloque para acceder al servicio.

Esta situación resulta incompatible con una concepción robusta del derecho a la autodeterminación informativa, pues limita significativamente la capacidad del titular para ejercer un control efectivo sobre sus datos personales. La problemática abarca relevancia en TikTok, donde el tratamiento de datos personales no se limita a la información

proporcionada directamente por el usuario, sino que comprende también datos inferidos a partir de sus hábitos de navegación, preferencias de consumo, tiempo de visualización, patrones de interacción y comportamiento digital. En este contexto, el consentimiento generalizado dificulta que el usuario conozca con precisión cuáles son los tratamientos concretos que autoriza y cuáles son las consecuencias derivadas de dicha autorización.

Cabe recordar que la protección de datos personales implica reconocer a los individuos un poder efectivo de control sobre la información que les concierne, permitiéndoles decidir sobre los usos específicos de sus datos y no simplemente aceptar tratamientos de manera genérica o indeterminada (Rodota, 2009). Bajo esta perspectiva, la autodeterminación informativa exige que el consentimiento sea suficientemente específico para que la persona pueda comprender y controlar cada una de las finalidades para las cuales será utilizada su información.

En ese sentido, la Autoridad Nacional de Datos Personales debería emitir lineamientos específicos que reconozcan expresamente la exigencia de granularidad del consentimiento en los entornos digitales. De esta forma, se establecería un marco de actuación a fin de que TikTok implemente un sistema de consentimiento granular basado en la separación de finalidades. Bajo este modelo, cada tratamiento de datos que exceda lo estrictamente necesario para la prestación del servicio debería requerir una autorización independiente, clara y específica. Así, el usuario podría aceptar determinadas finalidades y rechazar otras sin perder el acceso al servicio esencial de la plataforma.

La necesidad de establecer este criterio encuentra respaldo en estándares internacionales de protección de datos, es así que la European Data Protection Board, organismo que ha señalado que el consentimiento debe otorgarse de forma específica para cada finalidad de tratamiento y que los usuarios deben poder elegir separadamente entre distintas operaciones cuando éstas persigan objetivos diferentes (2020,17). Según dicho organismo, la agrupación de múltiples finalidades en una única solicitud de consentimiento afecta la libertad de decisión del titular y dificulta el ejercicio efectivo de sus derechos. También, las Directrices sobre Consentimiento elaboradas por el Article 29 Working Party precisan que la granularidad constituye una condición indispensable para la validez del consentimiento, pues garantiza que los interesados puedan autorizar determinados tratamientos sin verse obligados a aceptar otros que no resulten necesarios para la prestación del servicio (2018,10). Este criterio busca evitar que el consentimiento se convierta en una autorización general para cualquier forma de explotación de los datos personales.

En otras palabras, TikTok debería diferenciar, como mínimo, entre las siguientes categorías de tratamiento: (i) tratamiento necesario para la creación y gestión de la cuenta; (ii) personalización de contenidos y recomendaciones; (iii) segmentación publicitaria basada en el comportamiento del usuario; (iv) elaboración de perfiles predictivos e inferencias sobre intereses o preferencias; y (v) transferencia o compartición de datos con terceros para fines comerciales. Cada una de estas finalidades debería contar con mecanismos de aceptación independientes, claramente identificados y fácilmente modificables por el usuario en cualquier momento.

La necesidad de implementar este tipo de mecanismos se vuelve aún más evidente si se considera que el consentimiento informado atraviesa actualmente una crisis funcional en los

entornos digitales complejos. El desarrollo del Big Data, la inteligencia artificial y los sistemas de perfilamiento automatizado ha generado escenarios en los que los usuarios difícilmente pueden comprender la totalidad de los tratamientos realizados sobre sus datos personales ni prever las consecuencias futuras derivadas de ellos (Cotino, 2020). En consecuencia, la protección de los derechos fundamentales no puede depender exclusivamente de una aceptación genérica de términos y condiciones.

Desde el ordenamiento jurídico, la propuesta resulta plenamente compatible con el principio de finalidad recogido en el art. 6 de la LPDP. Dicho principio exige que los datos sean recopilados para fines determinados, explícitos y legítimos. Si las finalidades del tratamiento son múltiples y diferenciadas, el consentimiento también debe reflejar dicha diferenciación. De lo contrario, el titular no puede conocer con precisión qué usos específicos está autorizando ni ejercer un control efectivo sobre ellos. Así, la protección de datos personales constituye un derecho fundamental autónomo cuya finalidad principal es limitar el poder que ejercen entidades públicas y privadas sobre la información de los individuos, garantizando espacios reales de decisión y control por parte de los titulares de los datos (Praeli, 2015: 189). Precisamente, la granularidad del consentimiento fortalece esta dimensión garantista al devolver al usuario la capacidad de decidir de manera específica sobre cada tratamiento de su información personal.

Por todo lo anterior, la separación de finalidades y la implementación de mecanismos de consentimiento granular constituyen herramientas necesarias para fortalecer el derecho a la autodeterminación informativa frente a las prácticas de perfilamiento y segmentación publicitaria desarrolladas por plataformas digitales como Tik Tok. Junto con el desacoplamiento del servicio esencial y con mecanismos de transparencia algorítmica, estas medidas permiten superar las limitaciones del modelo tradicional basado en un consentimiento único y formal, promoviendo una protección más efectiva de los datos personales en el entorno digital.

VII. CONCLUSIONES:

- El consentimiento informado, piedra angular de la Ley N.° 29733, se enfrenta a una crisis estructural en entornos digitales caracterizados por la complejidad tecnológica y la asimetría informativa. Si bien la normativa exige que sea libre, previo, expreso e informado, la práctica revela que los usuarios aceptan políticas de privacidad extensas y técnicamente incomprensibles como condición necesaria para acceder al servicio. Este mecanismo de “tómalo o déjalo” convierte al consentimiento en un mero requisito formal que legitima tratamientos masivos de datos (perfilamiento, segmentación publicitaria, inferencias conductuales) sin que el titular comprenda realmente su alcance o pueda ejercer un control efectivo sobre su información. La autodeterminación informativa, entendida como el poder de disposición y control sobre los datos personales, se diluye frente a una aceptación automatizada y desinformada.

- El modelo de negocios de plataformas como Tiktok se sustenta en la extracción, análisis y explotación masiva de datos personales y conductuales, bajo la lógica del capitalismo de vigilancia. La información personal ya no es solo un atributo de la identidad, sino un activo comercial de alto valor que alimenta sistemas de

perfilamiento predictivo y publicidad hiper personalizada. Esta dinámica genera una asimetría estructural: mientras la plataforma posee un conocimiento detallado sobre el comportamiento del usuario y el funcionamiento de sus algoritmos, el individuo se encuentra en una posición de indefensión, sin herramientas efectiva para comprender cómo se construyen sus perfiles digitales ni para cuestionar las decisiones automatizadas que afectan su experiencia en la plataforma. El consentimiento, en este contexto, se convierte en un instrumento que legitima la explotación de datos sin ofrecer una contraprestación real en términos de control o transparencia.

- Los menores de edad, que constituyen una porción sustancial de la audiencia de Tik Tok, representan el caso más paradigmático de la insuficiencia del consentimiento informado. Si bien el artículo 1358 del Código Civil peruano habilita a los menores con discernimiento para celebrar actos vinculados a las necesidades ordinarias de su vida diaria, resulta jurídicamente insostenible equiparar estas transacciones cotidianas con el otorgamiento de consentimiento para tratamientos masivos y automatizados de datos personales. El perfilamiento algorítmico, la segmentación publicitaria y la elaboración de inferencias conductuales generan repercusiones complejas, transfronterizas y permanentes que escapan a la comprensión del menor e incluso de muchos adultos. Esta situación no solo evidencia la insuficiencia del consentimiento como mecanismo de protección, sino que plantea un serio cuestionamiento sobre la vulneración del principio del interés superior del niño y la necesidad de estándares de protección reforzados.

- El marco normativo peruano, sustentado en la Constitución y la LPDP, reconoce principios fundamentales como los de consentimiento, finalidad, proporcionalidad y transparencia. Sin embargo, su aplicación práctica frente a sistemas algorítmicos complejos presenta limitaciones significativas. La reciente actualización del Reglamento (Decreto Supremo N° 016-2024-JUS), al incorporar conceptos como la elaboración de perfiles y las evaluaciones de impacto, sienta una base para una supervisión más robusta, aunque se requiere un desarrollo interpretativo y, eventualmente, legislativo para que sea plenamente efectiva.

- La experiencia del derecho comparado, particularmente el GDPR y el Dictamen 8/2024 del EDPB, ofrece criterios valiosos para superar las deficiencias del modelo actual. Tendencias como la responsabilidad proactiva (*accountability*), la privacidad desde el diseño (*privacy by design*), la transparencia algorítmica y el consentimiento granular proporcionan un camino para fortalecer la protección de los usuarios en el Perú.

- Para superar la insuficiencia del consentimiento, se propone un mecanismo de protección integral basado en tres pilares interdependientes. En primer lugar, el desacoplamiento del servicio esencial, que garantice el acceso a las funcionalidades básicas de la plataforma sin la necesidad de aceptar el tratamiento de datos con fines de segmentación publicitaria, ofreciendo una alternativa equivalente y gratuita. En segundo lugar, el derecho a una explicación objetiva del tratamiento algorítmico, que exija a las plataformas proporcionar información individualizada y comprensible

sobre cómo se han utilizado los datos personales para mostrar un anuncio específico. En tercer lugar, la granularidad del consentimiento, que permita al usuario otorgar su autorización de manera separada y específica para cada finalidad de tratamiento, evitando la aceptación global e indivisible.

- La implementación efectiva de los mecanismos propuestos requiere un rol activo de la Autoridad Nacional de Protección de Datos Personales, en ejercicio de sus facultades supervisoras e interpretativas. Se recomienda la emisión de lineamientos, directrices u opiniones técnicas vinculantes que desarrollen los principios de servicio esencial sin perfilamiento, transparencia algorítmica específica y granularidad del consentimiento, brindando seguridad jurídica y guiando a las plataformas digitales hacia el cumplimiento de los estándares constitucionales y legales de protección de datos.

REFERENCIAS BIBLIOGRÁFICAS

Abrusio, J. (2024). The (In)Efficacy of Consent for the Processing of Personal Data.

https://www.humanitiesandrights.com/journal/index.php/har/article/view/133

Constitución Política del Perú. (1993).

Castro, K. (2017). La protección de datos personales y el consentimiento en entornos digitales. Revista Derecho PUCP.

Cortés, J. y Vizcaíno, A. (2025). Consumo fragmentado de marcas en TikTok: El impacto de la publicidad en la generación Alfa. Revista de Comunicación, 24(1), 109-126. https://revistadecomunicacion.com/index.php/rcom/es/article/view/3659

Cotino, L.(2020). *Inteligencia artificial, big data y aplicaciones contra la COVID-19: privacidad y protección de datos*. IDP. Revista de Internet, Derecho y Política, n.º 31, 2020, pp. 1-17. DOI: 10.7238/idp.v0i31.3244.

https://dialnet.unirioja.es/servlet/articulo?codigo=7633148&utm_source=chatgpt.com

Eguiguren, F. (2015). El derecho a la protección de datos personales como derecho fundamental autónomo. THEMIS Revista de Derecho, (67), 181-194.

https://revistas.pucp.edu.pe/index.php/themis/article/view/14462

European Data Protection Board. (2024). *Opinion 08/2024 on valid consent in the context of consent or pay models implemented by large online platforms*. https://www.edpb.europa.eu/system/files/2024-04/edpb_opinion_202408_consentorpay_en.pdf#8#1

Nissenbaum, H. (2010). *Privacy in context: Technology, policy, and the integrity of social life*. Stanford University Press
https://crypto.stanford.edu/portia/papers/privacy_in_context.pdf

Olivos, M. (2020). El derecho a la protección de datos personales en el Perú. IUS Revista de Investigación Jurídica. https://revistas.usat.edu.pe/index.php/ius/article/view/338

Pauner, C. (2023). *Transparencia algorítmica en los medios de comunicación y las plataformas digitales*. *Revista Española de la Transparencia, 17*, 107–136. https://doi.org/10.51915/ret.308

Piñar, J. (2005). *El derecho fundamental a la protección de datos personales. Algunos retos de presente y futuro*. *Asamblea. Revista Parlamentaria de la Asamblea de Madrid, 13*, 21–46. https://doi.org/10.59991/rvam/2005/n.13/604

Rodotà, S. (2009). *La vita e le regole. Tra diritto e non diritto* (ed. ampliata). Milano: Feltrinelli.
https://www.feltrinellieditore.it/opera/la-vita-e-le-regole-1-2-3/?utm_source=chatgpt.com

Rubio, M. (1999). Estudio de la Constitución Política de 1993 (Tomo I). Fondo Editorial PUCP.

Tribunal Constitucional del Perú. (2003). Sentencia recaída en el Expediente N.° 1797-2002-HD/TC. https://www.tc.gob.pe/jurisprudencia/2003/01797-2002-HD.html

Fuentes, J. & Sánchez, D. (2017). *Delimitación del derecho a elegir libremente entre productos y servicios*. **Derecho & Sociedad**, (49). Pontificia Universidad Católica del Perú https://revistas.pucp.edu.pe/index.php/derechoysociedad/article/view/19896?utm_source=chatgpt.com

Vicente-Fernández, P. y Díaz-Lucena, A. (2024). TikTok como herramienta de marketing digital: estudio de caso de la marca Freshly Cosmetics. Doxa Comunicación, 38, pp. 183-206.

https://doi.org/10.31921/doxacom.n38a1962.

Wang, Y. (2020). Humor and camera view on mobile short-form video apps influence user experience and technology-adoption technology-adoption intent, an example of TikTok (DouYin). Computers in Human Behavior, 110, 106373. https://doi.org/10.1016/j.chb.2020.106373.

Boza, B. (2004). Acceso a la información del Estado. *Marco legal y buenas prácticas*.

https://cendoc.esan.edu.pe/fulltext/e-documents/CAD/Libro_Acceso_Informacion.pdf

Huapaya, A. S. (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/29972

Angarita, N. R. (2003). El tratamiento de datos personales para fines estadísticos desde la perspectiva del gobierno electrónico. *Cuadernos de Derecho Público*.

https://revistasonline.inap.es/index.php/CDP/article/download/696/751

Gallego Fernández, L. D. (2015). El consentimiento en el derecho a la protección de datos.

https://repositorio.uniandes.edu.co/bitstreams/001b4a3f-ec09-4daa-857d-66b231d1c8c1/download