‘Biometría bajo la lupa: El Caso Mercado Libre Y Las Nuevas Reglas De Juego’

Departamento de Derecho de las Comunicaciones y Tecnologías de la Información.

Universidad Externado de Colombia

3 de Julio de 2025

Bogotá D.C., Colombia

Compilado por
Jaider Jael Morales Torres

Universidad Externado de Colombia

Calle 12 No. 1-17 Este
Bogotá D.C., Colombia

Teléfono: 282 60 66 Ext.1105, 1106
esdercom@uexternado.edu.co

INTRODUCCIÓN

El crecimiento acelerado de las plataformas digitales y el incremento de la actividad comercial en línea han convertido la verificación de identidad en un requisito casi esencial para asegurar la protección de los usuarios. No obstante, el empleo de tecnologías de autenticación fundamentadas en datos biométricos como la biometría facial supone desafíos éticos y jurídicos cada vez más difíciles, sobre todo porque son datos personales considerados sensibles y que requieren un grado superior de protección.

En este contexto, la reciente sanción impuesta por la Superintendencia de Industria y Comercio (SIC) a Mercado Libre reabre la discusión sobre los límites del uso de la biometría, las obligaciones que tienen las empresas frente a la recolección y tratamiento de esta información, y las posibles consecuencias regulatorias por incumplimiento. Este evento buscó ofrecer un análisis integral del caso concreto, explicar qué son y por qué importan los datos biométricos, revisar buenas prácticas y herramientas legales para implementar procesos de autenticación seguros, y reflexionar sobre los riesgos que conlleva el uso de estas tecnologías en el entorno digital.

Agenda del evento:

Instalación
Sandra Ortiz Laverde. Directora del Departamento de Derecho, Comunicaciones y Tecnologías de la Información de la Universidad Externado de Colombia.
Segmento 1: Presentación del caso de Mercado Libre y régimen de protección de datos personales vigente.
María del Pilar Cortés Rivas, abogada de la Universidad externado de Colombia y experta en datos personales.
Carolina García Molina, directora de Investigaciones de Protección de Datos de la Superintendencia de Industria y Comercio

Segmento 2: Análisis de los aspectos más relevantes de la sanción impuesta por la Superintendencia d Industria y Comercio
María del Pilar Cortés Rivas, abogada de la Universidad externado de Colombia y experta en datos personales.
Carolina García Molina, directora de Investigaciones de Protección de Datos de la Superintendencia de Industria y Comercio
Segmento 3: Preguntas del publico

INSTALACIÓN

La Dra. Sandra Ortiz Laverde inició la sesión con unas palabras de instalación que resaltaron la importancia del tema central: el régimen de protección de datos personales, a propósito de la reciente sanción impuesta por la Superintendencia de Industria y Comercio a una plataforma digital por el uso de biometría facial.

Durante la apertura, presentó a las dos expertas invitadas, destacando su amplia trayectoria en el sector privado y público, así como su labor en la asesoría legal. Indicó además que Carolina García Molina trabajó directamente en el área de protección de datos personales de la Superintendencia de Industria y Comercio, acumulando una experiencia significativa en la materia, incluida su participación en grupos de regulación del sector de telecomunicaciones. Además, resaltó que las expositoras son egresadas del posgrado del Departamento de Derecho, Comunicaciones y Tecnologías de la Información y destacó el valor de que fueran dos mujeres expertas las que lideraran esta conversación sobre biometría y datos personales.

Indicó que la sesión se dividiría en tres etapas principales: primero, una presentación general acerca del régimen de protección de datos personales vigente; segundo, un examen de los elementos más significativos de la sanción impuesta, incluyendo los criterios aplicados por la Superintendencia; y por último, un espacio de conversación enfocado en considerar el papel de las compañías del sector

privado, el espectro del uso de datos biométricos y los desafíos que representa la regulación actual.

Seguidamente, dio la Palabra a María del Pilar Cortés Rivas con el fin de que realizara la presentación del caso de Mercado Libre y del régimen de protección de datos personales vigente en Colombia.

La Dra. María del Pilar, primero reconoció que el evento permitiría evidenciar el debate y tener una conversación frente al tema que cobró mayor relevancia desde el mes de abril, cuando se conocieron algunas decisiones del ente regulador y vigilante, la SIC. Sostuvo que las decisiones trataron algunos temas de datos personales, en especial de la biometría.

Mencionó que el tema es muy importante para los asesores y quienes ejercen cargos como oficial de protección de datos personales dentro de las empresas. Seguidamente, explicó que antes de ver el caso concreto, se revisaría el marco legal de manera rápida con una pequeña enunciación de la normativa para que cuando se desarrollará el tema, los asistentes tuviesen una guía básica frente a este asunto, sin embargo, recomendó hacer una revisión detallada del tema.

Para iniciar con el marco normativo, indicó que respecto al tema de *habeas data* la constitución nacional en su artículo 15 habla de este derecho fundamental y de la responsabilidad o de la facultad que tenemos los colombianos de revisar nuestros datos, hacer consultas e incluso dar y retirar la autorización para que puedan tener acceso o no terceros a esa información. Recordó que siempre es importante que los dueños de los datos personales tengan en cuenta que son precisamente ellos los titulares y no como en algunos casos que parece que lo son las empresas.

Posteriormente, comentó que hace varios años, en el sector financiero existían riesgos de suplantación y no se tenía la posibilidad de hacer la revisión y validación frente a la información que estaba cursando en el sistema, ante lo cual, surgió la

primera norma, la Ley 1266 del 2008, que empezó a regular varios temas acerca de datos personales, respecto a qué podían o no hacer las entidades financieras con los datos y qué derechos tenían nosotros los usuarios frente a los temas de datos personales.

La expositora mencionó que previamente se tuvo también la Ley 527 de 1999 que fue de las primeras normas que empezó a hablar ya de temas tecnológicos, mensajes de datos, comercio electrónico, firma digital, certificación electrónica y comenzó a dar una aproximación los datos que consistían en esa información que viajaba en la red. También respecto a qué se entendía por información digital y cuál era la validación digital que podíamos tener. Resaltó que los conceptos que trajo esta ley fueron las primeras aproximaciones ya que hoy tenemos una validación, una autenticación y una identificación físicas.

Sobre la misma ley, sostuvo que en el contexto actual si se quiere adelantar algún trámite ante alguna autoridad, lo primero que se pide es identificarse con la cédula de ciudadanía, caso en el cual no hay ninguna situación en particular y simplemente se muestra el documento, pero esta norma empezó a indicar qué pasa cuando no se está en el medio físico, sino en el digital, en el comercio electrónico, cómo es en ese ámbito la firma, la aceptación etc. Así, los primeros vestigios de la regulación del comercio electrónico lo encontramos en esta Ley 527 de 1999.

Luego, trajo a colación la Ley 1581 del 2012, respecto de la cual sostuvo que puso en primer plano el tema de los datos, también destacó que dicha norma, viene de una regulación española que llevaba un tiempo de más en todo el desarrollo en temas de datos personales, pero en el contexto local, el legislador empezó a hacer unas aproximaciones en cuanto a conceptos de datos personales, responsabilidades de datos personales, deberes y otorgó unos tiempos a las empresas para que empezaran a implementar este cumplimiento.

Mencionó que algo importante de la norma, es que empezó a hablar de autorización, de consentimiento y comenzó a llamar la atención frente a que los datos personales no son un tema que pasaría desapercibido, sino que sería algo en lo que debían las empresas, empezar a enfocar su cuidado.

Seguidamente, realizó una exposición sobre los decretos reglamentarios y resaltó que con estos, empezó a tomar mucha más forma y cuerpo el tema de los datos personales, pues con el Decreto 1377 del 2013 y el Decreto 1074 del 2015 se empezó a tener una estructura más consolidada de la regulación de los datos personales, se incorporaron unas obligaciones, responsabilidades y principios, también la autorización y se regula cómo tiene que ser esa autorización, hay un aviso de privacidad y se regula cómo tiene que ser ese aviso de privacidad y el deber de información que tiene que ser veraz.

También, agregó que se asignaron unas competencias importantes en el Decreto 1074 de 2015, donde además se establecieron las responsabilidades y las competencias, los alcances que tiene la Superintendencia de Industria y Comercio como autoridad para poder investigar los casos que se presenten dentro de su jurisdicción frente al tema de datos personales.

Indicó que es importante conocer también las circulares, particularmente la circular única de la SIC que tiene un capítulo especial de datos personales, por lo cual se debe revisar con detalle las circulares y comunicados de la SIC. Con una revisión de todo lo enunciado, indicó que ya se puede contar con un marco general de lo que se debe tener en cuenta frente a datos personales y frente al cumplimiento de las obligaciones y responsabilidad.

A continuación, explicó que en el artículo tercero de la Ley 1581 se traen unas definiciones, aproximaciones de qué es un dato personal y sus clases, lo cual es relevante para el caso de Mercado Libre, porque se está hablando de datos sensibles. Explicó que la norma indica que los datos personales son aquella

información vinculada que permita determinar o identificar a un titular o al dueño de la información. Respecto a las clases, indicó que los hay públicos, semiprivados, privados y sensibles.

También, la norma define al responsable, que es la persona natural o jurídica que tiene a cargo decisiones sobre una base de datos, a su vez, habla de un encargado al que extiende esa responsabilidad, y se trata de una persona dentro de toda la cadena del tratamiento de los datos personales desde el almacenamiento, y respecto del cual se considera que si bien directamente no almacena o recopila el dato, tiene una responsabilidad en la cadena del uso del dato personal.

Por otra parte, señaló que la norma explica qué el titular es la persona cuyos datos personales son objeto de tratamiento, es decir, todos son titulares de datos personales. Unido a lo anterior, la ley establece quién es la autoridad que revisa los temas en lo relativo a datos personales, la Superintendencia de Industria y comercio.

En este punto, la expositora sostuvo que hay otros temas de la ley que son muy importantes, por una parte, el artículo 4 de la Ley 1581 establece unos principios rectores para el tema de datos personales, los cuales son: primero, legalidad, es decir, que todo debe estar establecido en la norma previamente; segundo, libertad, que la persona tiene libre disposición sobre quién maneja sus datos personales, quién almacena sus datos personales e incluso para pedirlos; el tercero, veracidad, que consiste en que el dato personal debe corresponder a la información cierta del titular.

Como cuarto principio, de transparencia, que se traduce en la posibilidad de saber quién accede a la información, quién dispone la información, qué información personal están recaudando y qué información están disponiendo. La Dra. María del Pilar, sostuvo que estos son los principales principios que rigen todos los temas de actividad frente al dato personal.

Mencionó que otro tema importante de la ley es el de la autorización, pues el consentimiento se vuelve fundamental para cualquier tratamiento de datos personales y dice la norma de manera clara que debe ser previo, expreso e informado. Además, le dice al responsable que debe guardar una copia, una prueba del momento en que recauda esa autorización. Sobre este tema, añadió que el Decreto 1377 expresa claramente qué debe contener la autorización y que es muy importante tener clara la finalidad, conocer para qué se va a utilizar, para qué se está recaudando, hasta cuándo se va a utilizar, quiénes van a tener acceso a esa información y con quiénes se va a compartir. Así pues, la norma es totalmente clara en cuanto al alcance de la autorización.

Seguidamente, la expositora comentó que el otro tema importante es el de las políticas de tratamiento de datos, puesto que, a pesar de la claridad de la norma, en la práctica muchas empresas no ajustan su conducta a las disposiciones de la ley. En ocasiones se piensa más en la estética que en el cumplimiento legal y desafortunadamente eso puede generar un incumplimiento normativo que se traduce por supuesto en sanciones en contra de la empresa o incluso en el peor de los casos, la imposibilidad de la empresa a seguir utilizando los datos personales por un tiempo determinado hasta tanto estén en cumplimiento que establece la norma, lo que genera un gran impacto por la importancia de las bases de datos.

Respecto al Decreto 1377 de 2013, la expositora expresó que también se consagra el mandato de que las empresas deben contar con políticas de tratamiento de datos con procedimientos internos organizados sobre datos personales, sobre avisos de privacidad. En sus contratos debe tener cláusulas claras y relativas acerca de los temas de datos personales. Así que, se debe tener en cuenta en los contratos, los procedimientos, los avisos de privacidad y las políticas de los avisos de videovigilancia deben estar de acuerdo con la norma. Recalcó que no se trata de cumplir por cumplir, sino que se logre llegar más allá del requerimiento mínimo.

Agregó que las políticas de tratamiento de datos deben estar de acuerdo con la naturaleza del negocio. Entonces, si se tiene un negocio digital no se puede tener condiciones de un procedimiento físico que no tiene nada que ver con el proceso propio de recaudo, almacenamiento, uso, disposición y conservación. Recordó que hay bases de datos que por su misma naturaleza requieren estar separadas, tener datos especiales, que haya una protección especial frente a datos sensibles y frente a los datos de los menores de edad.

Posteriormente, la Dra. María, trajo a colación el artículo 6 de la Ley 1581, respecto de los datos sensibles, en el que se prohíbe el tratamiento de datos sensibles salvo que el titular haya dado su autorización explícita a dicho tratamiento y el tratamiento sea necesario para salvaguardar el interés vital del titular, y si este se encuentra física o jurídicamente incapacitado, los representantes legales deberán otorgar su autorización del tratamiento.

Por otra parte, cuando el tratamiento sea efectuado en el curso de las actividades legítimas y con las debidas garantías por parte de una fundación, una ONG, una asociación o cualquier organismo sin ánimo de lucro cuya finalidad sea política, filosófica, religiosa o sindical, siempre que se refieran exclusivamente a sus miembros o a las personas que mantengan contactos regulares por razón de su finalidad, los datos no se podrán suministrar a terceros sin la autorización del titular.

Asimismo, explicó que cuando el tratamiento se refiera a datos que sean necesarios para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial o cuando el tratamiento tenga una finalidad histórica, estadística o científica, deberán adoptarse las medidas conducentes a la supresión de la identidad de los titulares y que esto debe leerse junto al artículo 2.2.2.25.2.3.del Decreto 1074 de 2015, que indica que en el tratamiento de los datos sensibles a qué se refiere el artículo quinto de la Ley 1581 de 2012, a excepción de los casos expresamente señalados en el artículo sexto de la misma ley, deberán cumplirse las siguientes obligaciones: primero, informar al titular quién por tratarse de datos sensibles no está obligado a

autorizar su tratamiento; segundo, informar al titular de forma explícita y previa y no podrá condicionarse para que suministre los datos personales sensibles. Señaló que esta última prohibición, se vuelve supremamente importante para el caso mercado libre.

Acto seguido, la Dra. María explicó el tema de la biometría, hizo énfasis en que primero es importante que en las empresas haya un experto que conozca, trabaje, maneje, direccione y organice y audite todos los procedimientos de biometría que se hacen dentro de las empresas. Sostuvo que se trata de un tema bastante técnico, pero para comprenderlo fácilmente, la biometría lo que hace es una captura que analiza esas características que ha capturado y las compara con datos almacenados previamente para determinar si hay coincidencia para permitir o denegar el acceso. Explicó que esas características pueden ser físicas como la huella dactilar, el reconocimiento facial o el iris.

A continuación, expuso para qué sirve el tema de la biometría, se utiliza para dos cosas, identificar y autenticar. Estas funciones suelen utilizarse para saber por ejemplo, si una transacción la está haciendo efectivamente quien es el titular.

Con el contexto normativo claro, la Dra. María, explicó el caso de mercado libre. Indicó que el expediente para la consulta es el 22301462 y que este proceso inició con una denuncia de un usuario, quien expresó que Mercado Libre quería obligarlo a registrar el reconocimiento facial en la aplicación de celular, no obstante que él tuvo su cuenta de Mercado Libre por años y podía verificar su identidad por medio del teléfono y correo electrónico, sin embargo, ahora Mercado Libre le quería obligar a que registrara su rostro para poder entrar a su cuenta.

El usuario también indicó que no quería usar el reconocimiento facial, ni que la empresa tuviese fotos de su rostro, sin embargo, no le permitieron entrar más a la cuenta si no registraba fotos de su cara. En su queja, el usuario relató que realizó varias solicitudes y le dijeron que no era posible desactivar esa opción. Así pues, su

petición fue que se le permitiera ingresar a su cuenta sin que tenga que otorgar sus datos de biometría.

La expositora señaló que la Superintendencia de Industria y Comercio mediante la resolución 160582 de 2025 profirió la decisión del caso Mercado Libre, donde hizo una revisión bastante juiciosa, de varias normativas relativas al tratamiento de datos, particularmente, el artículo 17 de la Ley 1581 de 2012, donde se encontró la mayoría de las posibles violaciones que se evidenciaron probatoriamente dentro de la investigación que hizo esta entidad.

Adicionalmente, hizo la claridad de que el artículo 12 de la misma norma, consagra algunos deberes de información que se tienen hacia los titulares, mientras que el artículo 17 dice cuáles son los deberes de los responsables de tratamiento de datos. En primera medida, este artículo, indica que se debe garantizar al titular en todo tiempo el pleno y efectivo derecho del habeas data.

La expositora mencionó que debe garantizar los derechos del titular, mediante la solicitud y conservación de los datos en las condiciones de la ley, conservar copia de la respectiva autorización otorgada por el titular, informar debidamente al titular sobre la finalidad de la recolección, garantizar que la información sea veraz, completa, exacta, actualizada, comprobable y comprensible, entre otras medidas.

A continuación, la oradora hizo relación en mayor detalle del artículo 12 de la Ley 1581, que trae el deber de informar al titular. El artículo señala que al momento de solicitar la autorización, debe informarle al titular, de manera clara y expresa el tratamiento al cual serán sometidos sus datos personales, la finalidad, el carácter facultativo de las respuestas que le sean hechas cuando versen sobre datos sensibles o sobre datos de niñas, niños y adolescentes, los derechos que le asisten como titular, la identificación, dirección física o electrónica y el teléfono del responsable. También, el responsable del tratamiento deberá conservar pruebas

del cumplimiento de lo previsto en el artículo y cuando el titular lo solicite debe entregarle copia de esto.

La Dra. María del Pilar, comentó que en la práctica, se ha encontrado con una buena cantidad de empresas que no solicitan la autorización o que a veces es la persona que está en la caja la que pone la autorización sin preguntar al titular, sobre lo que advirtió que se debe tener cuidado, ya que la autorización es del usuario o titular, no del funcionario que está en la caja, la ventanilla ni la persona de sistemas.

Con base en lo anterior, puso de presente que el argumento de la defensa en el caso mercado libre, consistió en que en ese contexto, hay unos temas de seguridad y suplantación que como empresa necesita garantizar y que a través de los procesos de verificación, se protegen los derechos de las personas que utilizan la plataforma, porque se necesita validar que el registro sea fidedigno y que no existan riesgos de suplantación de identidad y que no es cierto que se esté obligando a usar la biometría, puesto que se cuenta con una verificación en 2 pasos, se ofrece la opción de reconocimiento facial, pero puede hacerlo también con un QR y a través del autenticador de Google que puede hacer desde el teléfono, así que los usuarios cuentan con otros medios.

No obstante lo anterior, la SIC, realizó el proceso de verificar el paso a paso de cómo se hace la creación de la cuenta y cómo se entrega el dato personal en esta aplicación que utiliza Mercado Libre en este proceso de creación y validación de los titulares. Finalmente, hay una decisión a través de la Resolución 160582 de 2025 que le impuso una sanción de 214´405.120 COP. Recalcó que en esa resolución se encuentran cada uno de los cargos que en su momento generó la Superintendencia de Industria y Comercio y la explicación frente a los argumentos de la defensa de Mercado Libre y si logró o no acreditar estas circunstancias.

Expresó que la Superintendencia evidenció la violación de algunas de las prohibiciones de los responsables que consagra la ley, y tasó la sanción de acuerdo

con eso. Sin embargo, no solo impuso una sanción, sino que, además le impartió una orden administrativa consistente en la obligación de suprimir cualquier procedimiento en su aplicación o sitio web que condicione el acceso o creación de cuentas del usuario al suministro de datos biométricos. Para ello deberá ofrecer varias opciones que permitan a los titulares decidir el mecanismo de autenticación.

De manera seguida, la Dra. María del Pilar resaltó que en la asesoría de empresas que están relacionadas con el tema de SARLAFT y SAGRILAFT, la DIAN y la circular de la Superintendencia Financiera que establece unas obligaciones frente a estos temas de autenticación, validación, datos personales, se encuentra una confrontación con estas medidas ordenadas por la SIC, pues las empresas se plantean cómo hacer para cumplir entonces a la Superfinanciera.

La expositora concluyó su intervención con que a partir de la decisión, queda claro que hay una responsabilidad adicional por el tema de protección contra suplantación y otros riesgos asociados, sin embargo, la empresa puede utilizar otros mecanismos, que no sea solamente la recolección de datos biométricos a través de los datos sensibles. Y frente a las normas de protección al consumidor en el comercio electrónico y de SARLAFT y SAGRILAFT, DIAN etc. que prevén algunos lineamientos para el perfeccionamiento de la compraventa de bienes y servicios, así como la de verificar la identidad de las partes. Esa razón no se erige como justificación para condicionar, así sea de manera excepcional el uso o acceso de la cuenta de usuario al titular de proporcionar su información biométrica.

Con base en esto, la SIC ordenó a la sociedad Mercado Libre, implementar mecanismos que permitan verificar la plena identidad de sus suscriptores sin que esta derive en la exigencia inexorable de acceder a su registro facial y otros datos de biometría.

En este punto, la Dra. Sandra Ortiz tomó la palabra e indicó se proseguía a escuchar a la persona que lideró el tema desde la SIC, cuáles son sus aplicaciones y las

restricciones que dieron paso a esta sanción. Con esta introducción, dio paso a la Dra. Carolina García.

La Dra. Carolina García inició su intervención con la aclaración de que la decisión del caso Mercado Libre todavía no se encontraba en firme, pues se estaba surtiendo el proceso de apelación. Adicionalmente, indicó que, en su intervención en el evento, sería poco parcializada en cuanto a que a pesar de que la decisión definitiva no fue directamente suya, y que igualmente, ya salió de su oficina para el trámite del recurso de apelación ante el Delegado, esto le permitiría un mayor margen en sus comentarios.

Seguidamente, sostuvo que en el momento de abordar el caso, no se previó que tuviese tanto impacto la decisión, a pesar de que se venía teniendo una política interna de tratar de proteger a los titulares de la información en el tratamiento de sus datos sensibles y datos biométricos especialmente, de la mano con las políticas que el nuevo Delegado de la entidad ha querido gestionar y que la idea es hacer entender a los responsables y encargados y a los mismos titulares de información que el tema de la biometría tratándose como un dato sensible no es un tratamiento que debería adecuarse de manera general.

Explicó que dentro de la normativa que se tiene en Colombia, el tema del manejo de datos sensibles, debe ser excepcional, no general, y es uno de los pilares, no solamente de esta decisión sino que lo ha sido de otras decisiones que se están tomando con fundamento en la ley específicamente y en el comportamiento del responsable, con el fin de indicar por parte de la entidad de la autoridad de Protección de Datos, la existencia de unas normas que hay que cumplir, que se debe proteger al titular y hay que tomar las medidas adecuadas.

Señaló que en el tratamiento de los datos y más cuando se trata de este tipo de datos sensibles o biométricos y de menores, se debe tener una diligencia mucho mayor en el tratamiento de estos. Específicamente con esta decisión de Mercado

Libre, se buscó modular un poco la gestión que hacen algunas empresas, se quiere poner de presente que algunas empresas están tomando la biometría de manera muy general, con fundamento en el tema de evitar la suplantación de identidad.

Sin embargo, no se trata de que desde la entidad se esté en contra de ninguna medida que permita evitar un fraude o una suplantación a un titular, pero les interesa el titular y también la empresa que bajo un tema de suplantación también se ve afectada dentro de su actividad y dentro de sus patrimonios. Entonces no solamente es proteger de suplantación al titular, sino también a los responsables, pero hay que hacerlo de buena manera.

Indicó que para hacer esto bien, se tiene la Ley 1581 de 2012, un análisis constitucional por parte de la Corte de esta norma y decretos reglamentarios en donde se profundiza un poco más el cumplimiento de la ley. Así que se tienen las herramientas y deben usarse, recalcó que no se trata de impedir que exista tratamiento de datos biométricos, es hacerlo de manera adecuada. Con este fin, se quiso dar el mensaje de que se deben buscar otras alternativas que permitan llegar a esa misma finalidad sin incurrir incluso en una posible negligencia frente al tema de recolección de datos sensibles mediante dato biométrico.

Hizo un llamado a las empresas y entidades para que hagan esto adecuadamente, que revisen dentro de sus operaciones de qué manera ese dato sensible, biométrico, de menores y dato de cualquier tipo, es pertinente, necesario y conducente para la finalidad que persiguen. Se debe analizar si la biometría del rostro es necesaria o si no hay otro método a través del cual se pueda cumplir ese propósito específico.

Comentó que la decisión tomada en el caso Mercado Libre, estuvo muy encaminada a otras decisiones que se han tomado con otro tipo de datos, donde los responsables o encargados han sido de alguna forma muy inquisidores con el titular en el tema de su intimidad personal, incluso en el acceso a su dispositivo móvil para

poder recaudar sus fotos, recaudar sus documentos, recaudar su correo. Entonces, en la práctica se está desbordando el límite legal al punto de querer usar la biometría por todo y para todo.

Puso de presente también que este caso no ha sido el único, se han recibido varias quejas donde las personas manifiestan inconformidad porque no les gusta que les soliciten su biometría y se sienten inseguros a que se les vulnere la intimidad. Reflexionó en cuanto a que muchas veces, no se tiene esa confianza de dar datos, particularmente los biométricos, incluso para un tratamiento que quizá se requiera. Sostuvo que esto se debe a que muchas veces no hay una consciencia de que el titular tiene que ser debidamente informado, es decir, tiene que entender para qué es ese tratamiento y el responsable debe ser transparente en la manera en cómo esos datos se van a gestionar, respecto de lo que reconoció que fallan muchos responsables.

Hizo alusión a que en muchos casos, se pide una “autorización sombrilla” donde quieren incluir la autorización para muchas cosas, dentro de las cuales, tal vez el titular no está de acuerdo y no le han dado la opción de escoger qué tipo de autorización quiere dar.

En cuanto al proceso que llevó a la sanción, comentó que en la dirección de investigaciones de la SIC, se cuenta con un equipo multidisciplinario de abogados e ingenieros forenses y en este tipo de casos se hace un análisis bien minucioso frente a las aplicaciones móviles y la página de internet. Comentó que en el caso Mercado Libre, se hizo un recorrido del proceso de interacción del usuario con esta empresa y con sus aplicaciones y así identificar cuáles eran las falencias, lo que llevó a la decisión tomada.

A continuación, la Dra. Sandra Ortiz tomó la palabra e indicó que el sector financiero está utilizando también este tipo de procesos de verificación con biometría, teniendo en cuenta esto, preguntó cómo acompaña la SIC a las empresas en ese sistema de

recolección, cómo se está manejando y si hay una interacción entre Superintendencia Financiera y la SIC.

Carolina García respondió que en cuanto a la interacción entre la Superfinanciera y la SIC, si bien aún no hay una coordinación, se está tratando de hacer mesas de trabajo para que se pueda coordinar la labor, teniendo en cuenta que se percibe desde la SIC que efectivamente la Superfinanciera tiene su norma activa específica en temas de seguridad, en donde exige incluso la biometría o ciertos mecanismos en donde los titulares deciden.

Insistió en que se deben poner a disposición estos mecanismos alternativos, pero siempre se debe cumplir la Ley 1581 y que la biometría no sea la generalidad sino la excepción y que, en caso de usarla, sea con toda la conciencia y con toda la responsabilidad.

Por su parte, María del Pilar Cortés, dijo que las organizaciones a las que más puso en alerta la decisión fue las del sector Fintech, sector financiero y algunas de sector postal, porque algunos de sus servicios están muy relacionados con los temas de biometría, ya sea dactilar o facial, para efectos de verificación y validación de la identidad de las personas que están transando para brindar seguridad en temas de suplantación principalmente.

Sostuvo que en caso de hacer un cambio hacia otras alternativas, deberá haber un periodo de transición o haber algún tiempo en el que con un requerimiento previo se permita que las empresas amolden o reorganicen su situación interna en cuanto a sus sistemas porque esto requiere unos cambios estratégicos. La pregunta sería ¿cómo sería ese proceso de transición y cuál sería ese acompañamiento para que las empresas logren hacer esa transición?

Carolina García retomó la palabra y sostuvo que tenemos la norma desde el 2012 y la transición en este caso, sería por ejemplo administrativamente a través del

cumplimiento de una orden, por ejemplo, que la SIC otorgue un plazo específico para que ajusten sus procedimientos para dar cumplimiento a esa orden. Así mismo, indicó que desde la parte regulatoria, las circulares de la SIC están amparadas por la facultad de vigilancia y supervisión de las personas obligadas frente a esta entidad, bajo esa facultad, se dan pautas para que los vigilados cumplan la norma.

Por lo cual, ante la expedición de una eventual circular, se tendrá un período de ajuste por parte de la autoridad de protección de datos y las empresas tendrán que hacer una modulación. En este punto, se dio la palabra a los asistentes del evento para realizar preguntas, en primera medida, Luis Papagni preguntó ¿cómo se asegura que las plataformas ofrezcan alternativas reales y no condicionen el uso de datos biométricos? y ¿existen medidas de control o sanción para cuando un ciudadano pide retirar su consentimiento y pide eliminar sus datos biométricos?

Carolina García respondió que el tema de protección de datos es una obligación para el responsable y un deber para el usuario. Para el titular de la información, es la posibilidad de decir dentro de la libertad informática si quiero o no ese tratamiento de datos. Sin embargo, hay ocasiones en las que no podrá hacerse la supresión del dato por algunos motivos legales o contractuales y eso llevaría a que de alguna forma no haya responsabilidad por parte del responsable del tratamiento si no puede suprimir el dato por una condición legal o contractual.

Explicó que una vez cumplida la finalidad específica para la cual fue recaudado ese dato, ya no hay un deber legal o contractual que cumplir así que se debe eliminar esa información. Indicó que un ejemplo claro de esto es el caso de Mercado libre, donde el titular dijo que no quería que ellos tuvieran sus datos y no había en su momento una obligación legal o contractual de tenerlos.

Comentó también que la SIC ha encontrado en sus actuaciones, contratos y actos o negocios jurídicos en los que no solamente piden la autorización para el negocio como tal o para llevar a cabo ese esa ejecución contractual, sino para otros fines

distintos. Así, la diferencia será en el momento en que se haga un análisis de un caso concreto donde se informe la finalidad específica y si es una finalidad contractual o legal en donde el responsable tenga la obligación de suprimir o no el dato.

Con base en lo anterior, explicó que en el caso de Mercado Libre, la biometría no existió desde el comienzo y no era necesaria para el negocio porque el usuario ya tenía su cuenta, entonces se le solicitó un acceso adicional y le hicieron realizar ese registro de rostro para poder acceder a la plataforma cuando ya previamente estaba registrado y ya había podido ingresar y hacer sus transacciones dentro de la plataforma, entonces no había una razón por la cual no pudiera acceder por otro medio.

Respecto al segundo interrogante, María del Pilar dijo que los usuarios deben volverse muy vigilantes de este tipo de situaciones y que una vez se presenten, hay que ponerlas en conocimiento de la autoridad, también, que sería importante que se hagan unas campañas de educación por parte de la SIC y unas mesas de trabajo empresariales que permitan un cumplimiento real.

Carolina García por su parte, expresó que a través de la decisión estudiada, se busca instruir a las empresas y a los titulares respecto a que hay otros mecanismos más allá del dato biométrico y que no puede exigirse ni condicionarse absolutamente nada a la entrega de este.

Respecto a Mercado Libre, sostuvo que ellos mismos tienen otros mecanismos alternativos de autenticación. Por lo cual, desde la SIC, se están profiriendo decisiones administrativas en donde se dan órdenes muy concretas, a través de las cuales se orienta a la empresa a que establezca mecanismos alternativos dentro de los recursos con los que se cuente ya que estas alternativas deben ser definidas directamente por la empresa de acuerdo con sus posibilidades.

Adicionalmente, expresó que desde la entidad se tienen unas guías que aunque no son obligatorias, son recomendaciones, por ejemplo, hay una del tema de seguridad

y respecto a qué alternativas de implementación interna por parte de los responsables que podrían generar algún alivio para la entidad en cuanto al tratamiento de datos, no obstante, insistió en que no son ordenes de obligatorio cumplimiento.

La siguiente pregunta se enfocó en el tema de que hay fotos que son recolectadas por empresas de vigilancia para realizar el registro de acceso a un edificio, universidad, propiedad horizontal u otros espacios, y se trata de un dato biométrico. Se preguntó ¿La recolección y tratamiento debe realizarse teniendo en cuenta la guía sobre el tema de la SIC?

Carolina García indicó en primera medida que esa guía está en proceso de actualizar ciertas cosas. Adicionalmente, comentó que a través de la Oficina Asesora Jurídica de la Superintendencia y de algunas decisiones administrativas que han expedido en la dirección, se ha modulado un poco el tema de la fotografía en cuanto a que *per se* sea dato biométrico.

Explicó que la foto es biométrica o es un dato biométrico en tanto tenga una tecnología que permita la validación específica y exacta del titular, entonces no es cualquier foto que se tome sino que se trate de aquella que aplique mecanismos de autenticaciones que permitan individualizar totalmente a la persona, ahí en ese momento, el carácter biométrico de esa foto es de carácter sensible y cuando estemos fuera de este escenario, podrá tratarse de información semiprivada o pública, dependiendo el contexto.

Seguidamente, se recordó que la huella digital es un dato biométrico y el titular tiene la potestad de autorizar o no su tratamiento, pero que sin embargo, aseguradoras para un proceso de vinculación, exigen la huella digital o en pólizas de seguro se condicionan las coberturas a tener huella digital en un proceso de vinculación. Frente a esto se planteó: ¿Cómo se maneja ese tema, las aseguradoras tienen alguna norma especial que les permite exigir huella digital?

Carolina García explicó que en materia de aseguradoras, si la normativa especial exige el uso de la huella digital para fines específicos, dicho tratamiento se encuentra amparado bajo un marco de autorización legal. En estos casos, no se configuraría una vulneración a la Ley 1581 de 2012, siempre que el tratamiento se realice conforme a las condiciones y finalidades previstas. No obstante, subrayó que incluso cuando exista autorización normativa, el responsable del tratamiento debe cumplir con los principios generales de la ley, tales como transparencia, finalidad y seguridad, aplicables a lo largo de todo el ciclo del dato, desde su recolección hasta su eliminación.

María del Pilar Cortés complementó señalando que, en el caso de la regulación financiera, la exigencia de huella digital responde a obligaciones de identificación del cliente y a políticas internacionales en materia de prevención de lavado de activos y financiación del terrorismo (SARLAFT). Precisó que el tratamiento de datos sensibles no está prohibido, pero exige condiciones estrictas: autorización del titular, necesidad estricta, determinación clara y específica de la finalidad. Criticó la práctica de formular finalidades demasiado amplias en políticas de privacidad, insistiendo en que cuando se trata de datos sensibles debe definirse con precisión el uso que se dará a dicha información.

Ambas expertas coincidieron en la importancia del principio de responsabilidad demostrada, en virtud del cual las empresas deben garantizar que sus procesos de tratamiento de datos, especialmente los biométricos, sean robustos en términos técnicos, administrativos y de seguridad. García Molina destacó que, desde el punto de vista probatorio, el uso de datos biométricos implica un estándar más exigente, lo cual incrementa la carga de diligencia para los responsables.

En materia de propiedad horizontal, Carolina García señaló que el uso de biometría para el acceso a copropiedades se ha extendido de manera indiscriminada, generando numerosas quejas. Reiteró que corresponde al responsable del

tratamiento, en este caso, la copropiedad a través de sus órganos de decisión, determinar la pertinencia de dichos mecanismos, y advirtió que muchas veces no resulta ni necesario ni proporcional.

Por otra parte, resaltó la necesidad de que las empresas revisen de manera preventiva sus procesos de tratamiento de datos, eliminando autorizaciones innecesarias y prácticas invasivas, tales como el acceso a contactos, fotos o micrófonos de los usuarios sin justificación. Se enfatizó que tanto los responsables como los titulares deben ser conscientes de los límites en la recolección y uso de información.

Para finalizar, la Dra. Sandra Ortiz destacó la importancia de la formación académica en Derecho Informático y Protección de Datos, señalando que los programas de la Universidad Externado han sido pioneros y líderes en la región. Frente a esto, las expositoras coincidieron en que la universidad ha ofrecido un espacio de apoyo y acompañamiento académico sólido, con programas completos que integran a expertos del sector público y privado, lo cual ha fortalecido la discusión sobre la evolución de la protección de datos personales, especialmente frente a los retos de la Inteligencia Artificial y la Transformación Digital.

La jornada concluyó con el llamado a continuar generando espacios de capacitación, sensibilización y debate académico, así como a mantener la revisión crítica de las prácticas empresariales en materia de tratamiento de datos, en aras de garantizar los derechos de los titulares y fomentar la cultura de protección de los datos en el país.