REPUBLICA DE COLOMBIA

**MINISTERIO DE COMERCIO, INDUSTRIA Y TURISMO**
**SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO**

RESOLUCIÓN NÚMERO 71406 DE 2023

(15 de noviembre de 2023)

"*Por la cual se imparten unas órdenes administrativas*".

VERSIÓN ÚNICA

**Radicación**: 21-190473

**EL DIRECTOR DE INVESTIGACIÓN DE PROTECCIÓN DE DATOS PERSONALES**

En ejercicio de sus facultades legales, en especial las conferidas por el artículo 19 y los literales a) y b) del artículo 21, ambos de la Ley 1581 de 2012, y los numerales (5) y (9) del artículo 17 del Decreto 4886 de 2011, modificado por el artículo 7 del Decreto 092 de 2022, y

**CONSIDERANDO**

**PRIMERO:** Que la Dirección de Investigación de Protección de Datos Personales, mediante comunicación radicada bajo el número 21-190473- 2 del 26 de agosto de 2021, requirió a la sociedad **LINKEDIN IRELAND UNLIMITED COMPANY**, con el propósito de que informara lo siguiente:

> *"Hacemos referencia a la investigación realizada por Cybernews el pasado 06 de abril, respecto a la presunta exposición de información asociada a, aproximadamente, 500 millones de usuarios de Linkedin. Por tanto, en ejercicio de las funciones otorgadas por la Ley Estatutaria 1581 de 2012 a esta Superintendencia, como máxima autoridad de protección de datos personales en Colombia, nos permitimos solicitar atender los siguientes interrogantes:*
>
> *1) Con base en las indagaciones realizadas por ustedes, ¿se determinó si dentro de las cuentas expuestas, se encuentran datos personales de nacionales colombianos?*
>
> *2) En caso afirmativo, precisen ¿Qué datos personales privados, semiprivados y/o sensibles administrados por Linkedin fueron conocidos por terceros no autorizados?*
>
> *3) ¿Cuáles fueron las medidas adoptadas por la plataforma para mitigar los efectos de la exposición no controlada de los datos en la dark web, conforme a las investigaciones del sitio web Cybernews?*
>
> *4) ¿De acuerdo con el comunicado oficial de la plataforma, alojado en el vínculo https://news.linkedin.com/2021/april/an-update-from-linkedin, a qué tipo de perfiles se hace referencia con publicly viewable member profile/ miembros visibles públicamente? Señale cuál es el mecanismo utilizado para obtener la autorización de los titulares, cuya información se encuentra visible a través de los buscadores de la web.*
>
> *5) Informen, si a la fecha, cuentan con registros de reclamaciones presentadas por vulneración del derecho de hábeas data de titulares de cuentas colombianas, asociadas a este incidente de seguridad".*

**SEGUNDO:** Que mediante escrito radicado bajo el número 21-190743- -4 del 01 de febrero de 2022, la compañía **LINKEDIN IRELAND UNLIMITED COMPANY** atendió el requerimiento de información remitido por esta autoridad.

**TERCERO:** Que, con base en la referida comunicación, esta Dirección envió el requerimiento radicado bajo el número 21-190473 -5 del 09 de agosto de 2022, a través del cual solicitó que se informara lo que, a continuación se cita:

> *"1. En la respuesta allegada, la compañía afirma que no tiene un desglose por país de todos los usuarios de LinkedIn afectados. No obstante, es imperioso para esta Superintendencia, identificar la información afectada de Titulares ciudadanos o residentes en la República de Colombia.*

*Para ello, solicitamos que nos informen la cantidad exacta de cuentas asociadas a nacionales colombianos y/o residentes en Colombia, que quedaron expuestas con ocasión de los accesos a sus sistemas de información. Al respecto, informe los datos que fueron extraídos del sitio web de LinkedIn.*

*2. Informen si, a la fecha de recibo de esta comunicación se han recibido reclamaciones por parte de titulares, respecto a la exposición de sus datos personales.*

*3. El literal g) del artículo 4 de la Ley 1581 de 2012 "por la cual se dictan disposiciones generales para la protección de datos personales", contempla el Principio de Seguridad, según el cual "La información sujeta a Tratamiento por el Responsable del Tratamiento o Encargado del Tratamiento a que se refiere la presente ley, se deberá manejar con las medidas técnicas, humanas y administrativas que sean*
*necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento".*

*Conforme a lo descrito, ¿considera la compañía LinkedIn que el "scraping" es un "acceso no autorizado o fraudulento" a la información personal de los usuarios de su plataforma?*

*4. En el marco de la Política de Tratamiento de Datos Personales de LinkedIn vigente en el momento en el que sucedieron los hechos bajo estudio, la compañía:*

*a. ¿Permitía el "scraping" por parte de algún(os) tercero(s)? De ser así, ¿contaba con la autorización de los titulares de acuerdo con los estándares de la legislación nacional?*
*b. ¿Les informaba a los titulares sobre la práctica del "scraping" y la información que podría ser susceptible de ser recolectada a través de esta práctica?"*

**CUARTO:** Que, a la fecha de expedición de este acto administrativo, no obra en el expediente respuesta alguna por parte de la compañía **LINKEDIN CORPORATION**[1] frente a esta última comunicación. Al respecto, es oportuno señalar que la presente actuación administrativa, adelantada de manera oficiosa, tiene su origen en la brecha de seguridad por "*Data Scraping*"[2] que en su momento fuera confirmada por **LINKENDIN**, en la cual terceros ajenos a esa plataforma accedieron a la información de cuentas de usuario, sin que mediara autorización para el efecto.

Sobre el particular, es preciso señalar que la extracción masiva de Datos Personales se realiza normalmente por medios automatizados. Aquella práctica, denominada en inglés como "*web scraping*", ha sido identificada por las Autoridades de Protección de Datos Personales como un riesgo para el debido Tratamiento de la información personal. La capacidad de las tecnologías de extracción de datos para recopilar y tratar extensas cantidades de información de individuos en Internet plantea importantes preocupaciones, incluso cuando la información que se está extrayendo sea de acceso público.

De manera más amplia, los Titulares pierden el control cuando su información personal se extrae sin su conocimiento y en contra de sus expectativas. Por ejemplo, los extractores de datos pueden agregar y combinar datos extraídos de un sitio con otra información personal y utilizarla para fines inesperados. Esto puede socavar la confianza de los Titulares en los Responsables y Encargados del Tratamiento.

Además, incluso si los Titulares deciden suprimir/actualizar/rectificar su información de aquellas páginas con información de acceso público (redes sociales, plataformas digitales, páginas web, etc.), los extractores de datos pueden continuar utilizando y compartiendo la información que ya han extraído, limitando el control de las personas sobre su huella digital[3].

---

[1] De acuerdo con lo informado en la Política de Privacidad de LinkedIn, quien actúa como Responsable del tratamiento respecto a la información tratada por fuera de los países que conforman la Unión Europea, Espacio Económico Europeo y Suiza es la sociedad LinkedIn Corporation.
[2] "*El scraping de datos, de un modo general, se refiere a una técnica en la cual un programa informático extrae datos del resultado generado por otro programa. El scraping de datos se manifiesta normalmente en el scraping web, el proceso de utilizar una aplicación para extraer información valiosa de un sitio web".* Tomado de https://www.cloudflare.com.
[3] Cualquier publicación en internet viaja rápidamente y puede dejar una huella permanente. Es por esta razón que se debe ser cuidadoso con el tipo de información que se comparte en internet, pues los Datos de cada persona tienen valor y pertenecen únicamente a los Titulares de la información.

**QUINTO:** Que, de conformidad con lo expuesto, se procederá a hacer las siguientes:

## CONSIDERACIONES DE LA DIRECCIÓN DE INVESTIGACIÓN DE PROTECCIÓN DE DATOS PERSONALES

### I. Competencia de la Superintendencia de Industria y Comercio para ordenar las medidas que sean necesarias para hacer efectivo el derecho a debido Tratamiento de Datos Personales.

El artículo 19 de la Ley Estatutaria 1581 de 2012, establece que "*la Superintendencia de Industria y Comercio, a través de una Delegatura para la Protección de Datos Personales, ejercerá la vigilancia para garantizar que en el Tratamiento de datos personales se respeten los principios, derechos, garantías y procedimientos previstos en la presente ley*". El artículo 21, por su parte, faculta a esta entidad para, entre otras: "*b) Adelantar las investigaciones del caso, de oficio o a petición de parte y, como resultado de ellas, ordenar las medidas que sean necesarias para hacer efectivo el derecho de hábeas data*. *(…) e) Impartir instrucciones sobre las medidas y procedimientos necesarios para la adecuación de las operaciones de los Responsables del Tratamiento y Encargados del Tratamiento a las disposiciones previstas en la presente ley*; (…) f) *Solicitar a los Responsables del Tratamiento y Encargados del Tratamiento la información que sea necesaria para el ejercicio efectivo de sus funciones*."

Así las cosas, existen expresas y suficientes facultades legales para que esta Superintendencia pueda iniciar investigaciones, así como impartir órdenes o instrucciones.

### II. La Ley 1581 de 2012 es aplicable a LIKEDIN CORPORATION por cuanto, a través del sitio web "*LINKEDIN*" se recolectan datos personales en el territorio de la República de Colombia, por medio de *cookies* que instala en los equipos o dispositivos de las personas residentes o domiciliadas en Colombia.

Ordena la Constitución Política de Colombia, en su artículo 15, que en cualquier actividad que recaiga sobre datos personales se respete la libertad y demás garantías consagradas en esa norma. Así, es de vital importancia recordar que el caso bajo estudio hace referencia al cumplimiento de exigencias de naturaleza Constitucional referidas al derecho fundamental al debido tratamiento de los datos personales de los ciudadanos.

En efecto, el artículo 15 de la Constitución Política Nacional no solo establece que "*todas las personas (…) a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas*"[4], sino que es clara al exigir que:

> ***"En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución".*** (Destacamos y subrayamos).

Con fundamento en lo anterior, se promulga la Ley Estatutaria 1581 de 2012 que desarrolla, entre otras, el citado derecho constitucional de categoría fundamental. En el artículo 2 de la referida norma se dispone lo siguiente:

> "*La presente ley aplicará al tratamiento de datos personales efectuado en territorio colombiano o cuando al Responsable del Tratamiento o Encargado del Tratamiento no establecido en territorio nacional le sea aplicable la legislación colombiana en virtud de normas y tratados internacionales*".

El término "*Tratamiento*" no solo se menciona en el artículo 15[5] de la Constitución Política de la República de Colombia, sino que, es determinante para establecer el campo de aplicación de la citada disposición normativa, la cual lo define de la siguiente manera:

> ***"Artículo 3. Definiciones.*** *Para los efectos de la presente ley, se entiende por:*

---

[4] Constitución Política de Colombia. Artículo 15.

[5] El artículo 15 de la Constitución de la República de Colombia dice, entre otras, lo siguiente: "*Todas las personas tienen derecho a (…) conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en los bancos de datos y en archivos de entidades públicas y privadas. En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución".* (Subrayamos)

*(…)*

*g) **Tratamiento:** Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión."*

Así las cosas, la Ley Estatutaria 1581 de 2012 es aplicable, entre otras, cuando:

a. El Tratamiento lo realiza el Responsable o Encargado, domiciliados o no en territorio colombiano, que directa o indirectamente, a través de cualquier medio o procedimiento, físico o electrónico, recolecta, usa, almacena o trata Datos personales en el territorio de la República de Colombia. Las anteriores hipótesis son ejemplos de *"tratamiento* [sic] *de datos* [sic] *personales efectuado en territorio colombiano"* a que se refiere la parte primera del mencionado artículo 2.
b. El Responsable o el Encargado no está domiciliado en la República de Colombia ni realiza Tratamiento de Datos dentro del territorio colombiano. Pero, existen normas o tratados internacionales que los obliga a cumplir la regulación colombiana.

La Corte Constitucional, por su parte, en relación con el ámbito de aplicación de ese artículo señaló en la Sentencia C-748 de 2011[6]:

*"Para la Sala, esta disposición se ajusta a la Carta, pues amplía el ámbito de protección a algunos Tratamientos de datos personales que ocurren fuera del territorio nacional, en virtud del factor subjetivo. En un mundo globalizado en el que el flujo transfronterizo de datos es constante, **la aplicación extraterritorial de los estándares de protección es indispensable para garantizar la protección adecuada de los datos personales de los residentes en Colombia, pues muchos de los Tratamientos, en virtud de las nuevas tecnologías, ocurren precisamente fuera de las fronteras.** Por tanto, para la Sala se trata de una medida imperiosa para garantizar el derecho al habeas data"*[7]. (Subrayado fuera de texto).

Es importante señalar que, otras autoridades de protección de datos han concluido que las *cookies* son mecanismos que usan empresas extranjeras para instalarlas en los equipos de las personas de otros países y recolectar sus datos.

Frente a lo anterior, a finales de 2013 la Agencia Española de Protección de Datos (en adelante AEPD) concluyó lo siguiente con ocasión de una investigación que inició contra Google:

"*En todo caso, (…) **la entidad Google Inc. recurre a medios situados en el territorio español con el fin de captar información en nuestro territorio (utilizando, entre otros, los equipos de los usuarios residentes en España para almacenar información de forma local a través de cookies y otros medios, así como ejecutando código en dichos dispositivos**), sin que la utilización de tales equipos para la recogida de datos se realice exclusivamente con fines de tránsito por el territorio de la Unión Europea, es decir, no se trata de equipos de transmisión, sino que **dichos equipos se emplean para la recogida y tratamiento de los datos**"*[8] *(…)"*. (Destacamos).

---

[6] Cfr. Corte Constitucional. Sentencia C-748 de 2011. Disponible en: http://www.corteconstitucional.gov.co/relatoria/2011/c-748-11.htm
[7] Cfr. Corte Constitucional. Sentencia C-748 de 2011. Consideración 2.4.4.

[8] La AEPD concluyó lo siguiente: "*la Agencia Española de Protección de Datos también es competente para decidir sobre el tratamiento llevado a cabo por un responsable no establecido en territorio del Espacio Económico Europeo que ha utilizado en el tratamiento de datos medios situados en territorio español, por lo que debe concluirse, igualmente, que la LOPD es aplicable al presente supuesto y procedente la intervención de la Agencia Española de Protección de Datos, por virtud de lo dispuesto en el artículo 2.1.c) de la LOPD*" (AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. Resolución R/02892/2013 del 19 de diciembre de 2013. Procedimiento sancionador PS/00345/2013 instruido a las entidades Google Inc. y Google Spain, S.L. Madrid, España).
La parte pertinente de la regulación española - Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal- sobre su ámbito de aplicación dice lo siguiente:
"*Artículo 2 Ámbito de aplicación.*
*1. La presente Ley Orgánica será de aplicación a los datos de carácter personal registrados en soporte físico, que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los sectores público y privado.*
*Se regirá por la presente Ley Orgánica todo tratamiento de datos de carácter personal:*
*a) Cuando el tratamiento sea efectuado en territorio español en el marco de las actividades de un establecimiento del responsable del tratamiento.*
*b) Cuando al responsable del tratamiento no establecido en territorio español, le sea de aplicación la legislación española en aplicación de normas de Derecho Internacional público.*
*c) **Cuando el responsable del tratamiento no esté establecido en territorio de la Unión Europea y utilice en el tratamiento de datos medios situados en territorio español, salvo que tales medios se utilicen únicamente con fines de tránsito**. (…)".* (Destacamos).

En cuanto a las *web cookies*, el sitio web de **LINKEDIN** las define, en su Política de Cookies, así*:*

> *"Una cookie es un pequeño archivo colocado en tu dispositivo electrónico que habilita las funcionalidades de LinkedIn. Cualquier navegador que visite nuestros sitios puede recibir cookies nuestras o de terceros, como nuestros clientes, socios o proveedores de servicios. LinkedIn o terceros pueden colocar cookies en tu navegador cuando visitas sitios web que no son de LinkedIn que muestran anuncios o alojan nuestros complementos y etiquetas.*
>
> *Utilizamos dos tipos de cookies: persistentes y de sesión. Las cookies persistentes permanecen después de la sesión actual y se usan con muchos fines, como el de reconocerte como un usuario existente. De este modo, resulta más sencillo volver a LinkedIn e interactuar con nuestros Servicios sin tener que volver a iniciar sesión. Como las cookies persistentes permanecerán en tu navegador, LinkedIn las leerá cuando vuelvas a uno de nuestros sitios web o a un sitio de un tercero que utilice nuestros Servicios. Las cookies de sesión solo se almacenan durante el tiempo que dure la misma (normalmente, lo que dure la visita que estés realizando en ese momento a un sitio web o la sesión con el navegador)"*[9].

En este contexto, la Política de Privacidad alojada en el enlace: https://es.linkedin.com/legal/cookie-policy? del sitio web **LinkedIn** informa que utiliza múltiples modalidades de cookies, informando adicionalmente que "*Los terceros también pueden usar cookies en relación con nuestros Servicios externos, como los servicios publicitarios de LinkedIn. Los terceros pueden utilizar cookies para ayudarnos a proporcionar nuestros Servicios. También podemos trabajar con terceros para nuestros propios fines de marketing y para permitirnos analizar e investigar nuestros Servicios".*

Al respecto, se pueden visualizar las siguientes modalidades de *cookies* utilizadas por **LinkedIn**:

| Finalidad | Descripción |
|---|---|
| Autenticación | Utilizamos cookies y tecnologías similares para reconocerte cuando visitas nuestros Servicios.<br><br>Si has iniciado sesión en LinkedIn, estas tecnologías nos ayudan a mostrarte la información adecuada y a personalizar tu experiencia de acuerdo con tu configuración. Por ejemplo, las cookies permiten a LinkedIn identificarte y verificar tu cuenta. |
| Seguridad | Utilizamos cookies y tecnologías similares para que tus interacciones con nuestros Servicios sean más rápidas y seguras.<br><br>Por ejemplo, utilizamos cookies para activar y respaldar nuestras funciones de seguridad, mantener la seguridad de tu cuenta y detectar actividades fraudulentas e infracciones de nuestras Condiciones de uso. |

[9] Obtenido de la Política de Cookies alojada en el enlace https://es.linkedin.com/legal/cookie-policy?

| | |
|---|---|
| Preferencias, funcionalidades y servicios | Utilizamos cookies y tecnologías similares para habilitar la funcionalidad de nuestros Servicios, como ayudarte a rellenar formularios de nuestros Servicios con mayor facilidad y proporcionarte funciones, información y contenido personalizado junto con nuestros complementos. También utilizamos estas tecnologías para recordar información sobre tu navegador y tus preferencias.<br>Por ejemplo, las cookies pueden decirnos qué idiomas prefieres y cuáles son tus preferencias de comunicación. También podemos utilizar el almacenamiento local para acelerar la funcionalidad del sitio. |
| Contenido personalizado | Utilizamos cookies y tecnologías similares para personalizar tu experiencia en nuestros Servicios.<br><br>Por ejemplo, podemos utilizar cookies para recordar búsquedas anteriores, de modo que, cuando vuelvas a utilizar nuestros Servicios, podamos ofrecerte información adicional relacionada con tu búsqueda anterior. |
| Complementos dentro y fuera de LinkedIn | Utilizamos cookies y tecnologías similares para habilitar los complementos de LinkedIn tanto dentro como fuera de los sitios de LinkedIn.<br><br>Por ejemplo, nuestros complementos, incluido el botón «Solicitar con LinkedIn» o el botón «Compartir», pueden encontrarse en LinkedIn o en sitios de terceros, como los sitios de nuestros clientes y socios. Nuestros complementos utilizan cookies y otras tecnologías para proporcionar análisis y reconocerte en LinkedIn y en sitios de terceros. Si interactúas con un complemento (por ejemplo, haciendo clic en «Solicitar»), este utilizará cookies para identificarte e iniciar tu solicitud.<br><br>Puedes obtener más información sobre los complementos en nuestra Política de privacidad. |
| Publicidad | Las cookies y las tecnologías similares nos ayudan a mostrarte publicidad relevante de forma más eficaz, tanto dentro como fuera de nuestros Servicios, y a medir el rendimiento de estos anuncios. Utilizamos estas tecnologías para obtener más información sobre si se te ha mostrado el contenido o si alguien que visualizó un anuncio volvió más tarde y llevó a cabo alguna acción (por ejemplo, descargar documentación o realizar una compra) en otro sitio. Asimismo, nuestros socios o proveedores de servicios pueden usar estas tecnologías para determinar si hemos mostrado un anuncio o una publicación y qué resultados obtuvo, o para obtener información sobre cómo interactúas con ellos.<br><br>También podemos colaborar con nuestros clientes y socios para mostrarte un anuncio dentro o fuera de los sitios web de LinkedIn, como después de visitar un sitio web o una aplicación de un cliente o socio. Estas tecnologías nos ayudan a proporcionar información adicional a nuestros clientes y socios.<br><br>Para obtener más información sobre el uso de cookies con fines publicitarios, consulta las Secciones 1.4 y 2.4 de la Política de privacidad.<br><br>Como se indica en la Sección 1.4 de nuestra Política de privacidad, fuera de los Países designados, también recopilamos (o terceros a los que recurrimos recopilan) información sobre tu dispositivo (por ejemplo, ID del anuncio, dirección IP, sistema operativo e información del navegador) cuando no utilizas nuestros Servicios, para ofrecer a nuestros Miembros anuncios relevantes y entender mejor su eficacia.<br><br>Para obtener más información, consulta la Sección 1.4 de la Política de privacidad. |
| Análisis e investigación | Las cookies y las tecnologías similares nos ayudan a obtener más información sobre el rendimiento de nuestros Servicios y complementos en diferentes ubicaciones.<br><br>Tanto nosotros como nuestros proveedores de servicios utilizamos estas tecnologías para comprender, mejorar e investigar productos, funciones y servicios, incluso mientras navegas por nuestros sitios o cuando accedes a LinkedIn desde otros sitios, aplicaciones o dispositivos. Tanto nosotros como nuestros proveedores de servicios utilizamos estas tecnologías para determinar y medir el rendimiento de los anuncios o las publicaciones dentro y fuera de LinkedIn, así como para saber si has interactuado con nuestros sitios web, contenidos o correos electrónicos, y proporcionar análisis basados en esas interacciones.<br><br>También utilizamos estas tecnologías para proporcionar información adicional a nuestros clientes y socios como parte de nuestros Servicios.<br>Si eres miembro de LinkedIn, pero has cerrado la sesión de tu cuenta en un navegador, LinkedIn puede continuar registrando tus interacciones con nuestros Servicios en ese navegador hasta el vencimiento de la cookie para generar análisis de uso asociados a nuestros Servicios. Podemos compartir estos análisis de forma conjunta con nuestros clientes. |

Frente a la recolección de información a través de *Cookies*, **LinkedIn** informa a sus usuarios, a través de la citada Política de Privacidad, que:

> *"Tal y como se describe en nuestra Política de cookies, utilizamos cookies y tecnologías similares (por ejemplo, balizas web y etiquetas de anuncios) para recopilar información (por ejemplo, identificadores de dispositivos) para reconocerte a ti y/o a tu dispositivo o dispositivos en los diferentes Servicios y dispositivos. También permitimos que otras personas usen cookies en el modo descrito en nuestra Política de cookies. Si no resides en uno de los Países designados, recopilamos (o terceros a los que recurrimos recopilan)* ***información sobre tu dispositivo (por ejemplo, ID del anuncio, dirección IP, sistema operativo e información del navegador****) para ofrecer a nuestros Miembros anuncios relevantes y entender mejor su eficacia. Más información. También puedes marcar la opción de autoexclusión para que no utilicemos la información de las cookies ni de tecnologías similares para hacer un seguimiento de tu comportamiento en otros sitios web para la publicidad de terceros. Los Visitantes disponen de controles aquí".* (destacamos)

Entonces, es dable concluir sin lugar a duda, que una *cookie* es un mecanismo que se instala en los equipos o dispositivos (bien sea celular, computador portátil u otro) de las personas residentes o domiciliadas en la República de Colombia, con el objetivo de recolectar algunos de sus datos personales. Por tanto, el sitio web https://www.linkedin.com, propiedad de la compañía **LINKEDIN CORPORATION**, realiza tratamiento de datos personales en el territorio colombiano, sujeto a las disposiciones de la Ley 1581 de 2012.

## III. LINKEDIN CORPORATION tiene la obligación de cumplir la Legislación colombiana, así como las órdenes y requerimientos de esta autoridad, en cumplimiento de la Ley 1581 de 2012.

La regulación sobre tratamiento de datos personales debe aplicarse al margen de los procedimientos, metodologías o tecnologías que se utilicen para recolectar, usar o tratar ese tipo de información. La Ley colombiana permite el uso de tecnologías para tratar datos pero, al mismo tiempo, exige que se haga de manera respetuosa del ordenamiento jurídico. Quienes crean, diseñan o usan "innovaciones tecnológicas" deben cumplir todas las normas sobre tratamiento de datos personales.

Entonces, es importante decir que nuestra Constitución Política Nacional establece:

> Artículo 4 *"(…) Es* ***deber de los nacionales y de los extranjeros*** *en Colombia acatar la Constitución y las leyes, y respetar y obedecer a las autoridades"*[10]*.*
>
> Artículo 333 *"(…) La actividad económica y la iniciativa privada son libres, dentro de los límites del bien común. Para su ejercicio, nadie podrá exigir permisos previos ni requisitos, sin autorización de la ley. La libre competencia económica es un derecho de todos que supone responsabilidades*. **La empresa, como base del desarrollo, tiene una función social que implica obligaciones**". (Destacamos).

Entonces, es la misma Constitución Política la que dispone el cumplimiento de la normatividad a los extranjeros que estén en este territorio. La cual, además, incluye el sometimiento a la ley en general, así como a las órdenes de autoridades administrativas, entre otras.

## IV. El respeto por las leyes en el ciberespacio.

En el ciberespacio no desaparecen ni disminuyen los derechos de las personas. El ciberespacio ha sido caracterizado por ser un escenario global no delimitado por fronteras geográficas en donde las actividades suceden dentro de la arquitectura tecnológica de Internet. Aunque se trata de un "mundo virtual", sus ciudadanos son millones de personas reales ubicadas en prácticamente cualquier lugar del "mundo físico", cuyas actividades tienen impacto o consecuencias en el "mundo real".

A pesar de que el campo de acción de Internet desborda las fronteras nacionales, para la Corte Constitucional el nuevo escenario tecnológico y las actividades en Internet no se sustraen del respeto de los mandatos constitucionales. Por eso, concluyó esa Corporación que "*en Internet (…) puede haber una realidad virtual pero ello no significa que los derechos, en dicho contexto, también lo sean. Por el contrario, no son virtuales: se trata de garantías expresas por cuyo goce efectivo en el*

---

[10] "*Dicho reconocimiento genera al mismo tiempo la responsabilidad en cabeza del extranjero de atender cabal y estrictamente el cumplimiento de deberes y obligaciones que la misma normatividad consagra para todos los residentes en el territorio de la República pues, así lo establece, entre otras disposiciones, el artículo 4o. inciso segundo de la Carta (…)".* Corte Constitucional, Sentencia C-1259 de 2001

*llamado "ciberespacio" también debe velar el juez constitucional*"[11]. Recalca dicha Corporación que, "*nadie podría sostener que, por tratarse de Internet, los usuarios sí pueden sufrir mengua en sus derechos constitucionales*"[12].

De otra parte, **LinkedIn** informa en su sitio web que cuenta con, alrededor de 850 millones de cuentas de usuarios en 200 territorios[13], incluyendo a Colombia, razón por la cual se puede colegir que esta tiene la obligación Constitucional y Legal de garantizarles a los nacionales colombianos el debido tratamiento de sus datos personales y el correcto ejercicio de sus derechos fundamentales en el ciberespacio.

## V. Sobre el Tratamiento de Datos Personales por parte de LinkedIn

Con la finalidad de entender qué información es tratada por el sitio web y para qué finalidades, la Dirección De Investigación de Protección de Datos Personales ha procedido a revisar la información que dispone la Política de Privacidad del sitio web **LinkedIn** en los siguientes términos[14]:

| Categoría | Descripción |
|---|---|
| ***Registro*** | *Para crear una cuenta, debe proporcionar datos que incluyan su nombre, dirección de correo electrónico y / o número de teléfono móvil, y una contraseña. Si se registra para un Servicio premium, deberá proporcionar información de pago (por ejemplo, tarjeta de crédito) y facturación.* |
| ***Perfil*** | *Usted tiene opciones sobre la información en su perfil, como su educación, experiencia laboral, habilidades, foto, ciudad o área y endosos. No tiene que proporcionar información adicional en su perfil; sin embargo, la información del perfil le ayuda a obtener más de nuestros Servicios, incluida la ayuda a los reclutadores y las oportunidades comerciales para encontrarlo. Es su elección si desea incluir información confidencial en su perfil y hacer pública esa información confidencial. No publique ni agregue datos personales a su perfil que no desee que estén disponibles públicamente.* |
| ***Publicación y carga*** | *Recopilamos datos personales de usted cuando los proporciona, publica o carga en nuestros Servicios, como cuando completa un formulario (por ejemplo, con datos demográficos o salario), responde a una encuesta o envía un currículum vitae o completa una solicitud de empleo en nuestros Servicios. Si opta por importar su libreta de direcciones, recibimos sus contactos (incluida la información de contacto que su proveedor de servicios o aplicación agregó automáticamente a su libreta de direcciones cuando se comunicó con direcciones o números que aún no están en su lista).*<br><br>*Si sincroniza sus contactos o calendarios con nuestros Servicios, recopilaremos su libreta de direcciones y la información de las reuniones del calendario para seguir haciendo crecer su red sugiriendo conexiones para usted y otros, y proporcionando información sobre eventos, por ejemplo, horarios, lugares, asistentes y contactos.*<br><br>*No tiene que publicar o cargar datos personales; aunque si no lo hace, puede limitar su capacidad para crecer y comprometerse con su red a través de nuestros Servicios.* |
| ***Contenido y Noticias*** | *Usted y otros pueden publicar contenido que incluya información sobre usted (como parte de artículos, publicaciones, comentarios, videos) en nuestros Servicios. También podemos recopilar información pública sobre usted, como noticias y logros profesionales, y ponerla a disposición como parte de nuestros Servicios, incluso, según lo permita su configuración, en notificaciones a otros de menciones en las noticias.* |
| ***Información de contacto y calendario*** | *Recibimos datos personales (incluida información de contacto) sobre usted cuando otros importan o sincronizan sus contactos o calendario con nuestros Servicios, asocian sus contactos con perfiles de miembros, escanean y cargan tarjetas de visita o envían mensajes utilizando nuestros Servicios (incluidas invitaciones o solicitudes de conexión). Si usted u otras personas optan por sincronizar cuentas de correo electrónico con nuestros Servicios, también recopilaremos información de "encabezado de correo electrónico"* |

[11] Corte Constitucional. Sentencia C-1147 del 31 de octubre de 2001. Magistrado Ponente: Dr. Manuel José Cepeda Espinosa
[12] Corte Constitucional. Sentencia C-1147 del 31 de octubre de 2001. Magistrado Ponente: Dr. Manuel José Cepeda Espinosa
[13] De acuerdo con la información alojada en el enlace https://about.linkedin.com/es-es
[14] Obtenido del sitio web: https://www.linkedin.com/legal/privacy-policy?src=direct%2Fnone&veh=direct%2Fnone#data

| | |
|---|---|
| | *que podemos asociar con los perfiles de los Miembros.* |
| ***Socios*** | *Recibimos datos personales (por ejemplo, su cargo y dirección de correo electrónico del trabajo) sobre usted cuando utiliza los servicios de nuestros clientes y socios, como empleadores o posibles empleadores y sistemas de seguimiento de solicitantes que nos proporcionan datos de solicitud de empleo.* |
| ***Empresas relacionadas y otros servicios*** | *Recibimos datos sobre usted cuando utiliza algunos de los otros servicios proporcionados por nosotros o nuestras filiales, incluido Microsoft. Por ejemplo, puede optar por enviarnos información sobre sus contactos en aplicaciones y servicios de Microsoft, como Outlook, para mejorar las actividades de redes profesionales en nuestros Servicios.* |
| ***Uso del Servicio*** | *Registramos datos de uso cuando visita o utiliza nuestros Servicios, incluidos nuestros sitios, aplicaciones y tecnología de plataforma, como cuando ve o hace clic en contenido (por ejemplo, video de aprendizaje) o anuncios (dentro o fuera de nuestros sitios y aplicaciones), realiza una búsqueda, instala o actualiza una de nuestras aplicaciones móviles, comparte artículos o solicita empleos. Utilizamos inicios de sesión, cookies, información del dispositivo y direcciones de protocolo de Internet ("IP") para identificarlo y registrar su uso.* |
| ***Cookies y tecnologías similares*** | *Como se describe con más detalle en nuestra Política de cookies, utilizamos cookies y tecnologías similares (por ejemplo, píxeles y etiquetas de anuncios) para recopilar datos (por ejemplo, ID de dispositivo) para reconocerlo a usted y a su(s) dispositivo(s) en, apagado y en diferentes servicios y dispositivos donde ha interactuado con nuestros Servicios. También permitimos que otros utilicen cookies como se describe en nuestra Política de cookies. Si se encuentra fuera de los Países designados, también recopilamos (o confiamos en otros que recopilan) información sobre su dispositivo cuando no ha interactuado con nuestros Servicios (por ejemplo, ID de anuncio, dirección IP, sistema operativo e información del navegador) para que podamos proporcionar a nuestros Miembros anuncios relevantes y comprender mejor su efectividad. Más información. Puede optar por no participar en nuestro uso de datos de cookies y tecnologías similares que rastrean su comportamiento en los sitios de otros para la orientación de anuncios y otros fines relacionados con los anuncios. Para los visitantes, los controles están aquí.* |
| ***Su dispositivo y ubicación*** | *Cuando visita o abandona nuestros Servicios (incluidos algunos complementos y nuestras cookies o tecnología similar en los sitios de otros), recibimos la URL tanto del sitio del que proviene como del sitio al que va y la hora de su visita. También obtenemos información sobre su red y dispositivo (por ejemplo, dirección IP, servidor proxy, sistema operativo, navegador web y complementos, identificador y características del dispositivo, ID de cookies y / o ISP, o su operador de telefonía móvil). Si utiliza nuestros Servicios desde un dispositivo móvil, ese dispositivo nos enviará datos sobre su ubicación en función de la configuración de su teléfono. Le pediremos que se suscriba antes de usar GPS u otras herramientas para identificar su ubicación precisa.* |
| ***Mensajes*** | *Recopilamos información sobre usted cuando envía, recibe o interactúa con mensajes en relación con nuestros Servicios. Por ejemplo, si recibe una solicitud de conexión de LinkedIn, rastreamos si ha actuado en consecuencia y le enviaremos recordatorios. También utilizamos tecnología de escaneo automático en los mensajes para apoyar y proteger nuestro sitio. Por ejemplo, utilizamos esta tecnología para sugerir posibles respuestas a los mensajes y para administrar o bloquear contenido que viole nuestro Acuerdo de usuario o las Políticas de la comunidad profesional de nuestros Servicios.* |

De igual forma, se encontró que el sitio web **LinkedIn** utiliza de la siguiente manera la información recolectada de los Titulares:

| Finalidad | Descripción |
|---|---|
| ***Cómo utilizamos sus datos*** | *La forma en que usemos sus datos personales dependerá de los Servicios que utilice, cómo los use y las elecciones que realice en su configuración. Utilizamos los datos que tenemos sobre usted para proporcionar y personalizar nuestros Servicios, incluso con la ayuda de sistemas automatizados e inferencias que hacemos, para que nuestros Servicios (incluidos los anuncios) puedan ser más relevantes y útiles para usted y otros.* |
| ***Manténgase conectado*** | *Nuestros Servicios le permiten mantenerse en contacto y al día con colegas, socios, clientes y otros contactos profesionales. Para ello, puedes "conectarte" con los profesionales que elijas y que también deseen* |

| | |
|---|---|
| | *"conectarte" contigo. Sujeto a su configuración y la de ellos, cuando se conecte con otros Miembros, podrá buscar las conexiones de los demás para intercambiar oportunidades profesionales.* |
| ***Manténgase informado*** | *Nuestros Servicios le permiten mantenerse informado sobre noticias, eventos e ideas sobre temas profesionales que le interesan y de profesionales que respeta. Nuestros Servicios también le permiten mejorar sus habilidades profesionales o aprender otras nuevas. Utilizamos los datos que tenemos sobre usted (por ejemplo, los datos que proporciona, los datos que recopilamos de su compromiso con nuestros Servicios y las inferencias que hacemos de los datos que tenemos sobre usted), para personalizar nuestros Servicios para usted, como recomendar o clasificar contenido y conversaciones relevantes en nuestros Servicios (…).* |
| ***Carrera*** | *Nuestros Servicios le permiten explorar carreras, evaluar oportunidades educativas y buscar, y ser encontrado, oportunidades de carrera. Su perfil puede ser encontrado por aquellos que buscan contratar (para un trabajo o una tarea específica) o ser contratado por usted. Utilizaremos sus datos para recomendar trabajos o aprendices, mostrarle a usted y a otros contactos profesionales relevantes (por ejemplo, que trabajan en una empresa, en una industria, función o ubicación o tienen ciertas habilidades y conexiones).* |
| ***Productividad*** | *Nuestros Servicios le permiten colaborar con colegas, buscar clientes potenciales, clientes, socios y otras personas con las que hacer negocios. Nuestros Servicios le permiten comunicarse con otros Miembros y programar y preparar reuniones con ellos. Si su configuración lo permite, escaneamos los mensajes para proporcionar "bots" o herramientas similares que faciliten tareas como programar reuniones, redactar respuestas, resumir mensajes o recomendar los próximos pasos.* |
| ***Servicios Premium*** | *endemos Servicios premium que brindan a nuestros clientes y suscriptores funciones y herramientas de búsqueda personalizadas (incluidas alertas de mensajería y actividad) como parte de nuestras soluciones de talento, marketing y ventas. Los clientes pueden exportar información limitada de su perfil, como nombre, titular, empresa actual, título actual y ubicación general (por ejemplo, Dublín), como administrar clientes potenciales o talento, a menos que opte por no participar. No proporcionamos información de contacto a los clientes como parte de estos Servicios premium sin su consentimiento. Los clientes de Servicios Premium pueden almacenar información que tienen sobre usted en nuestros Servicios premium, como un currículum vitae o información de contacto o historial de ventas. Los datos almacenados sobre usted por estos clientes están sujetos a las políticas de esos clientes. Otros servicios empresariales y características que utilizan sus datos incluyen TeamLink y Elevate (promoción social de contenido).* |
| ***Comunicaciones*** | *Nos pondremos en contacto con usted a través de correo electrónico, teléfono móvil, avisos publicados en nuestros sitios web o aplicaciones, mensajes a su bandeja de entrada de LinkedIn y otras formas a través de nuestros Servicios, incluidos mensajes de texto y notificaciones push. Le enviaremos mensajes sobre la disponibilidad de nuestros Servicios, seguridad u otros problemas relacionados con el servicio. También enviamos mensajes sobre cómo usar nuestros Servicios, actualizaciones de red, recordatorios, sugerencias de trabajo y mensajes promocionales de nosotros y nuestros socios. Puede cambiar sus preferencias de comunicación en cualquier momento. Tenga en cuenta que no puede optar por no recibir nuestros mensajes de servicio, incluidos los avisos legales y de seguridad.* |
| ***Publicidad*** | *Le mostraremos anuncios llamados contenido patrocinado que se parecen al contenido no patrocinado, excepto que están etiquetados como publicidad (por ejemplo, como "anuncio" o "patrocinado"). Si realiza una acción social (como dar me gusta, comentar o compartir) en estos anuncios, su acción se asocia con su nombre y otros pueden verla, incluido el anunciante. Sujeto a su configuración, si realiza una acción social en los Servicios de LinkedIn, esa acción puede mencionarse con anuncios relacionados. Por ejemplo, cuando le gusta una empresa, podemos incluir su nombre y foto cuando se muestra su contenido patrocinado.* |

De este modo, es claro que **LinkedIn** tiene realiza tratamiento de datos personales, en calidad de Responsable del tratamiento, calidad que le impone el cumplimiento de las obligaciones que en ese sentido, contempla nuestra Legislación.

**VI. La existencia de riesgos para los derechos y libertades de los individuos frente al tratamiento de sus Datos personales.**

Los datos personales pueden ser recogidos por diferentes fuentes, entre ellas: formularios, *cookies*, aplicaciones móviles, sitios web, redes sociales, registros públicos, programas de fidelización de clientes, etc. Todas estas formas de recolección, entre otras, son manifestaciones de: 1) Datos personales suministrados directamente por los titulares, 2) Datos personales recolectado en cumplimiento de un requisito legal, 3) Datos personales recopilados automáticamente con el uso de un servicio o producto (por ejemplo, datos de transacciones, direcciones IP, datos de ubicación), y 4) Datos personales inferidos mediante el Tratamiento y análisis de los datos suministrados por los individuos o recopilados con el uso del servicio o producto. Estos datos, sin lugar a dudas, también son de gran interés para terceros que no han sido autorizados para el Tratamiento de dicha información.

Si un dato personal es conocido, accedido o sustraído por terceros no autorizados, por ejemplo, piratas cibernéticos, se constituye en sí mismo como un riesgo para los derechos y libertades de los individuos, de gravedad y probabilidades variables. Considerando la cantidad y sensibilidad de la información personal que es recolectada en el ciberespacio mediante diversos mecanismos, procesos y tecnologías, la Corte Constitucional en Sentencia C-748 de 2011 subrayó el deber de los Responsables del Tratamiento de reforzar sus medidas de seguridad para proteger la información personal de los Titulares. Lo anterior como resultado de que "*el mal manejo de la información puede tener graves efectos negativos, no sólo en términos económicos, sino también en los ámbitos personales y de buen nombre"*[15].

**VII. Del deber de conservar la información bajo condiciones de seguridad.**

La seguridad de la información es una condición crucial del Tratamiento de Datos personales. Recolectada la información, esta debe ser objeto de medidas de diversa índole para evitar situaciones indeseadas que puedan afectar los derechos de los titulares y de los mismos Responsables y Encargados del Tratamiento. El acceso, la consulta y el uso no autorizado o fraudulento, así como la manipulación y pérdida de la información son los principales riesgos, pero no los únicos, que se quieren mitigar a través de medidas de seguridad de naturaleza humana, física, administrativa y/o técnica.

La seguridad de la información ha sido una preocupación del legislador colombiano y la Corte Constitucional. Esta última concluyó que, "*debe reiterarse que el manejo de información no pública debe hacerse bajo todas las medidas de seguridad necesarias para garantizar que terceros no autorizados puedan acceder a ella. De lo contrario, tanto el Responsable como el Encargado del Tratamiento serán los responsables de los perjuicios causados al Titular*"[16].

Las técnicas para la extracción y obtención de valor de datos públicamente accesibles están en constante evolución. De ahí que, la seguridad de los datos es una responsabilidad dinámica y la vigilancia por parte de todos los actores es fundamental.

La extracción masiva de Datos Personales se realiza normalmente por medios automatizados. Aquella práctica, denominada en inglés como "*web scraping",* ha sido identificada por las Autoridades de Protección de Datos Personales como un riesgo para el debido Tratamiento de la información personal. La capacidad de las tecnologías de extracción de datos para recopilar y tratar extensas cantidades de información de individuos en Internet plantea importantes preocupaciones, incluso cuando la información que se está extrayendo sea de acceso público.

Para el efecto, la Superintendencia de Industria y Comercio, en su rol de Autoridad Nacional de Protección de Datos Personales, suscribió una declaración conjunta con otras autoridades de protección de datos sobre esta materia[17]. Dentro de las preocupaciones que dicha declaración pone de presente para el debido Tratamiento de Datos Personales, son las siguientes:

---

[15] República de Colombia. Corte Constitucional. Sentencia C-748 del 6 de octubre de 2011. Considerando 2.6.5.2.7

[16] Corte Constitucional. Sentencia C-748 del 6 de octubre de 2011.

[17] El documento oficial se encuentra disponible para su visualización en el enlace https://ico.org.uk/media/about-the-ico/documents/4026232/joint-statement-data-scraping-202308.pdf

1. **Ataques cibernéticos dirigidos.** Por ejemplo, la información de identidad y contacto extraída que se publica en "foros de piratería" puede ser utilizada por actores maliciosos en ataques de ingeniería social dirigidos o ataques de *phishing*.
2. **Suplantación.** Los datos extraídos pueden utilizarse para enviar solicitudes fraudulentas de préstamos o tarjetas de crédito, o para suplantar a la persona creando cuentas falsas en redes sociales.
3. **Monitoreo, perfilamiento y vigilancia de individuos.** Los datos extraídos pueden utilizarse para generar bases de datos de reconocimiento facial y proporcionar acceso no autorizado a terceros.
4. **Marketing directo no deseado.** Los datos extraídos pueden incluir información de contacto que se puede utilizar para enviar mensajes de marketing no solicitados a granel.

Ahora bien, dado que ninguna única medida de seguridad protegerá adecuadamente, contra todos los posibles daños a los Titulares asociados con la extracción de datos, los Responsables y Encargados del Tratamiento de aquellas páginas con información de acceso público (redes sociales, plataformas digitales, páginas web, etc.), deben implementar medidas técnicas, humanas y administrativas para mitigar los riesgos. Aquellas medidas pueden incluir, pero no limitarse, a las siguientes:

- Designar un equipo y/o roles específicos dentro de la organización para identificar e implementar controles para proteger contra la extracción de datos, monitorearla y responder a las actividades de extracción.
- Limitar la "velocidad de acceso" a otros perfiles por parte de una cuenta a un número determinado de visitas por hora o día, y limitar el acceso si se detecta actividad inusual.
- Supervisar la rapidez y agresividad con la que una nueva cuenta comienza a buscar otros usuarios. Si se detecta una actividad anormalmente alta, esto podría ser indicativo de un Tratamiento sospechoso.
- Tomar medidas para detectar a los extractores de datos identificando patrones de actividad de "bots5". Por ejemplo, se pueden detectar un grupo de direcciones IP sospechosas al monitorear desde dónde se está accediendo a una plataforma utilizando las mismas credenciales desde múltiples ubicaciones. Esto sería sospechoso si estos accesos ocurren en un corto período de tiempo.
- Tomar medidas para verificar si un extractor de datos es un "bot", por ejemplo, mediante el uso de CAPTCHAs, y bloquear la dirección IP donde se identifica la actividad de extracción de datos.
- Cuando se sospecha y/o confirma la extracción de datos, tomar medidas legales apropiadas, como el envío de cartas de "Cese y Desistimiento", exigir la eliminación de la información extraída, obtener confirmación de la eliminación y tomar otras medidas legales para hacer cumplir los términos y condiciones que prohíben la extracción de datos.

Por su parte, esta Autoridad ha sido enfática en afirmar que, bajo el ordenamiento jurídico de nuestro país, la información personal que es "*públicamente disponible*", "*accesible al público*" no es, *per se*, información "*de naturaleza pública*". **El hecho de que estén disponibles en internet no significa que cualquier persona puede tratarlos sin autorización previa, expresa e informada del Titular del Dato**. Recolectar datos personales privados, semiprivados o sensibles en internet no legitima al recolector para apropiarse de dicha información y hacer lo que quiera con la misma.

Por su parte, la seguridad de los datos personales no se limita a situaciones de infiltración o burla de las medidas de seguridad que han implementado los Responsables y Encargado del Tratamiento. La Ley 1581 de 2012 va más allá porque exige lo siguiente:

> "***ARTÍCULO 4o. PRINCIPIOS PARA EL TRATAMIENTO DE DATOS PERSONALES****. En el desarrollo, interpretación y* ***aplicación*** *de la presente ley, se aplicarán, de manera armónica e integral, los siguientes principios:*
>
> *(…)*
>
> *g) Principio de seguridad: La información sujeta a Tratamiento por el Responsable del Tratamiento o Encargado del Tratamiento a que se refiere la presente ley, se deberá manejar con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros* ***evitando*** *su adulteración, pérdida, consulta, uso o* ***acceso no autorizado o fraudulento****;*
>
> *(…)*

> ***ARTÍCULO 17. DEBERES DE LOS RESPONSABLES DEL TRATAMIENTO****. Los Responsables del Tratamiento deberán cumplir los siguientes deberes, sin perjuicio de las demás disposiciones previstas en la presente ley y en otras que rijan su actividad:*
>
> *(…)*
> *d) Conservar la información bajo las condiciones de seguridad necesarias para* ***impedir su*** *adulteración, pérdida, consulta, uso o* ***acceso no autorizado*** *o fraudulento;*
>
> *(…)*
>
> ***ARTÍCULO 18. DEBERES DE LOS ENCARGADOS DEL TRATAMIENTO****. Los Encargados del Tratamiento deberán cumplir los siguientes deberes, sin perjuicio de las demás disposiciones previstas en la presente ley y en otras que rijan su actividad:*
>
> *(…)*
>
> *b) Conservar la información bajo las condiciones de seguridad necesarias para* **impedir** *su adulteración, pérdida, consulta, uso o* ***acceso no autorizado*** *o fraudulento (…)".*
>
> (Subrayado y negrita fuera de texto).

Nótese que **la redacción del principio de seguridad tiene un criterio eminentemente preventivo**, lo cual obliga a los Responsables y Encargados del Tratamiento a adoptar medidas apropiadas y efectivas para **evitar** afectaciones a la seguridad de la información. **Es preciso aclarar que la implementación de las medidas de seguridad por parte de los Responsables y Encargados del Tratamiento no está supeditada o condicionada a que exista un daño o perjuicio de los derechos o intereses que se buscan proteger con la Ley 1581 de 2012**. El solo hecho de tratar datos personales es suficiente. Una interpretación en sentido contrario no solo iría en contra de la naturaleza preventiva que se deriva expresamente de los textos legales citados, sino que privaría a los colombianos de la capacidad de exigir a los Responsables y Encargados que aseguren un nivel adecuado de protección en relación con sus datos.

**VIII. De la facultad que tiene la Superintendencia de Industria y Comercio para emitir órdenes en relación con el debido Tratamiento de Datos Personales.**

Ley Estatutaria 1581 de 2012 expresamente faculta a esta entidad para emitir órdenes o impartir las instrucciones que considere necesarias para que el Tratamiento de Datos personales se realice conforme con lo dispuesto en la ley. En el artículo 19 de esta ley, se le otorgó competencia a esta entidad, a través de la Delegatura para la Protección de Datos Personales, para ejercer: *"(…) la vigilancia necesaria para garantizar que en el tratamiento [sic] de datos [sic] personales se respeten los principios, derechos, garantías y procedimientos previstos en la presente ley*."

Asimismo, su artículo 21 determina cuáles funciones ejercerá la Superintendencia de Industria y Comercio, en virtud de la competencia conferida por el artículo 19 mencionado:

> *a. "Velar por el cumplimiento de la legislación en materia de protección de datos [sic] personales;*
>
> *b. "Adelantar las investigaciones del caso, de oficio o a petición de parte y, como resultado de ellas,* ***ordenar las medidas que sean necesarias para hacer efectivo el derecho de hábeas [sic] data****. Para el efecto, siempre que se desconozca el derecho, podrá disponer que se conceda el acceso y suministro de los datos [sic], la rectificación, actualización o supresión de los mismos;*
>
> *(…)*
>
> *e.* ***"Impartir instrucciones sobre las medidas y procedimientos necesarios para la adecuación de las operaciones de los Responsables del Tratamiento*** *y Encargados del Tratamiento a* ***las disposiciones previstas en la presente ley****;".* (Destacamos).

No sobra traer a colación que, el artículo 21 fue declarado exequible por la Corte Constitucional mediante la Sentencia C-748 de 2011, la cual en su numeral 2.20.3, expresa:

> "*Esta disposición enlista las funciones que ejercerá la nueva Delegatura de protección de datos personales. Al estudiar las funciones a ella asignadas, encuentra esta Sala que todas*

*corresponden y despliegan los estándares internacionales establecidos sobre la autoridad de vigilancia. En efecto, desarrollan las funciones de vigilancia del cumplimiento de la normativa, de investigación y sanción por su incumplimiento, de vigilancia de la transferencia internacional de datos* ***y de promoción de la protección de datos****."*. (Destacamos).

Así, la ley colombiana faculta a la Superintendencia de Industria y Comercio no solo para emitir órdenes o instrucciones sino para exigir el debido Tratamiento de los Datos personales a compañías como la investigada.

**SEXTO:** Sin perjuicio de todo lo anterior, destacamos las siguientes **CONCLUSIONES**:

1. El sitio web de LinkedIn recolecta la siguiente información: "*nombre, dirección de e-mail o número móvil (…) información de pago (por ejemplo, la tarjeta de crédito) (…) educación, experiencia laboral, aptitudes, una fotografía"*.
2. El sitio web de **LinkedIn** emplea diversas tecnologías para recolectar y almacenar la información, entre las que se incluyen *cookies*, *balizas web* y *etiquetas de anuncios.*
3. El sitio web de LinkedIn usa *"cookies"* para recolectar o tratar datos personales en el territorio de la República de Colombia. Por ende, debe cumplir la Ley Estatutaria 1581 de 2012 y sus normas reglamentarias.

   En otras palabras, el tratamiento de datos personales que realiza el sitio web de **LinkedIn** está sujeto a la legislación de la República de Colombia, toda vez que recolecta información de ciudadanos y residentes que se encuentran en el territorio nacional. Así las cosas, la Ley Estatutaria 1581 de 2012 es aplicable al sitio web de **LinkedIn** porque acopia o captura Datos Personales por medio de cookies que instala en dispositivos móviles y ubicados en la República de Colombia**.**

4. La seguridad de la información es una condición crucial del tratamiento de datos personales. Una vez recolectados deben ser objeto de medidas de diversa índole para evitar situaciones indeseadas que pueden afectar los derechos de los titulares.
5. **LinkedIn** ha reconocido algunas fallas de seguridad y ha adoptado medidas para subsanarlas. No obstante, conforme a lo observado en la respuesta al requerimiento obrante en el expediente, aún subsisten algunas falencias. Dado lo anterior, esta Entidad considera necesario emitir órdenes administrativas de carácter preventivo para garantizar el principio y el deber de seguridad.

**SÉPTIMO:** Una orden administrativa no es una sanción, sino una medida necesaria para la adecuación de las actividades u operaciones de los Responsables del Tratamiento a las disposiciones de la regulación colombiana sobre protección de datos personales. Las sanciones por infringir la Ley Estatutaria 1581 de 2012 *-multas, suspensión de actividades, cierre temporal o definitivo-* están previstas en el artículo 23 de dicha norma. Allí se puede constatar que las órdenes no son sanciones.

**OCTAVO:** Que para garantizar el debido tratamiento de los datos de las personas residentes o domiciliadas en la República de Colombia es necesario emitir varias órdenes a las compañías **LINKEDIN CORPORATION** y **LINKEDIN IRELAND UNLIMITED COMPANY**.

En mérito de lo expuesto, este Despacho.

**RESUELVE**

**ARTÍCULO 1. ORDENAR** a **LINKEDIN CORPORATION** y **LINKEDIN IRELAND UNLIMITED COMPANY,** (en adelante **LINKEDIN**), implementar medidas y procedimientos para la adecuación de sus operaciones en la República de Colombia a las disposiciones de la Ley 1581 de 2012, las cuales deberán contener, como mínimo los siguientes estándares:

1) Mejorar o robustecer las medidas de seguridad que ha implementado a la fecha de expedición de la presente resolución para garantizar la seguridad de los Datos personales, evitando su: i) acceso no autorizado o fraudulento; ii) uso no autorizado o fraudulento; iii) consulta no autorizada o fraudulenta; iv) adulteración o v) pérdida.

2) Desarrollar, implementar y mantener un programa integral de seguridad de la información, que garantice la seguridad, confidencialidad e integridad de los Datos personales, evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento. El programa deberá constar por escrito, ser sujeto a pruebas periódicas para evaluar su efectividad e indicadores de cumplimiento y tener en cuenta, como mínimo, lo siguiente: a) Los principios rectores establecidos en la Ley 1581 de 2012 y los deberes que de ellos se derivan;

a) El tamaño y la complejidad de las operaciones de **LinkedIn;**
b) La naturaleza y el ámbito de las actividades de **LinkedIn;**
c) La cantidad de Titulares;
d) La naturaleza de los datos personales;
e) El tipo de tratamiento de los Datos personales;
f) El alcance, contexto y fines del Tratamiento;
g) Las actualizaciones o cualquier tipo de modificación de la plataforma de LinkedIn, sus productos cualquier otra forma en que LinkedIn utilice, recopile, comparta o trate los datos recolectados;
h) El acceso a los Datos personales por parte de los empleados, contratistas y en general los colaboradores de **LinkedIn**;
i) El uso de los Datos personales de los usuarios por terceros, entre ellos, aliados comerciales, empresas asociadas y desarrolladores de aplicaciones, si aplica;
j) El uso innovador o aplicación de nuevas soluciones tecnológicas;
k) Los riesgos internos y externos para la seguridad, confidencialidad y disponibilidad de los Datos personales; y
l) Los riesgos para los derechos y libertades de los Titulares.

3) Desarrollar, implementar y mantener un programa de gestión y manejo de incidentes de seguridad en datos personales, que contemple procedimiento para información sin dilación indebida a esta Superintendencia de Industria y Comercio y a los Titulares de cuando se presenten incidentes que afecten la confidencialidad, integridad y disponibilidad de los datos personales.

4) Desarrollar, implementar y mantener un programa de capacitación y entrenamiento rutinario para sus empleados y contratistas sobre su política de seguridad de la información, su política de gestión de incidentes de seguridad de datos y su Política de Tratamiento de Datos personales (o privacidad).

5) Poner en marcha un sistema de monitoreo permanente para verificar si, en la práctica, sus medidas de seguridad son útiles, suficientes o si están funcionando correctamente. En caso de que ello no sea así, adoptar las medidas necesarias para garantizar la seguridad de la información.

6) **LinkedIn** deberá efectuar una auditoría independiente, dentro de los cuatro (4) meses siguientes a la ejecutoria del presente acto administrativo, y cada año después de dicha fecha durante los próximos cinco (5) años, certificar a esta entidad que cuenta con las medidas técnicas, humanas, administrativas, contractuales y de cualquier otra naturaleza que sean necesarias para otorgar seguridad a los datos personales evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.

**ARTÍCULO 2: LinkedIn** deberá cumplir lo ordenado en esta resolución dentro de los cuatro (4) meses siguientes a la ejecutoria del presente acto administrativo y acreditar ante la Dirección de Investigaciones de Protección de Datos Personales de la Superintendencia de Industria y Comercio las medidas y procedimientos adoptados dentro de los cinco (5) días siguientes al vencimiento de dicho término.

**Parágrafo primero:** Para demostrar el cumplimiento, **LinkedIn** deberá remitir, al finalizar dicho plazo, una certificación emitida por una entidad o empresa, nacional o extranjera, independiente, imparcial, profesional y especializada que acredite que se han implementado las medidas ordenadas por esta Dirección y que estas se encuentran operando con suficiente efectividad para proporcionar el grado de seguridad que exige el principio y deber de seguridad de la Ley Estatutaria 1581 de 2012 respecto de los Datos personales.

**Parágrafo segundo**: La entidad o empresa que emita el certificado será seleccionada por **LinkedIn** pero debe ser un tercero cuya gestión esté libre de todo conflicto de interés que le reste independencia y sea ajena a cualquier tipo de subordinación respecto de **LinkedIn**.

**Parágrafo tercero:** La entidad o empresa certificadora deberá ser autorizada por la autoridad competente del país de su domicilio, sólo en el caso que la regulación correspondiente exija dicha autorización para poder emitir certificaciones. Si en dicho país no se exige lo anterior, bastará con que aquella sea independiente, imparcial, profesional y especializada en temas de seguridad de la información.

**ARTÍCULO 3. NOTIFICAR** el contenido de la presente resolución a **LinkedIn**, informándole que contra el presente acto administrativo procede recurso de reposición ante el Director de Investigación de Protección de Datos Personales y de apelación ante el Superintendente Delegado para la Protección de Datos Personales, dentro de los **diez (10)** días siguientes a la diligencia de notificación.

**ARTÍCULO 4:** La Superintendencia de Industria y Comercio se permite recordar que los canales habilitados para que los investigados ejerzan sus derechos, den respuesta a requerimientos, interpongan recursos, entre otros, son:

- Correo Superindustria: contactenos@sic.gov.co

- Sede Principal: Carrera 7 No. 31A - 36, Pisos 3 y 3A, en la ciudad de Bogotá, de lunes a viernes de 8:00 a.m. a 4:30 p.m.

**NOTIFÍQUESE Y CÚMPLASE**

Dada en Bogotá D. C., 15 de noviembre de 2023

**El DIRECTOR DE INVESTIGACIÓN DE PROTECCIÓN DE DATOS PERSONALES,**

**CARLOS ENRIQUE SALAZAR MUÑOZ**

Proyectó: Laura Rodríguez
Revisó: Carlos Salazar
Aprobó: Carlos Salazar

**NOTIFICACIÓN:**

| | |
|---|---|
| Sociedades: | **LINKEDIN CORPORATION**<br>**LINKEDIN IRELAND UNLIMITED COMPANY** |
| Identificación: | No se cuenta con identificación |
| Correo electrónico: | lberger@linkedin.com |
| Dirección: | AV 1000 W. MAUDE AVENUE SUNNYVALE, CA 94085 EE. UU. |
| Ciudad: | SUNNYVALE-CALIFORNIA-ESTADOS UNIDOS DE AMERICA |