REPUBLICA DE COLOMBIA

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

RESOLUCIÓN NÚMERO _____58834_____ DE 2023

(28 de septiembre 2023)

Por la cual se resuelve un recurso de apelación

Radicación 18-153189

VERSIÓN ÚNICA

EL SUPERINTENDENTE DELEGADO PARA LA PROTECCIÓN DE DATOS PERSONALES (E)

En ejercicio de sus facultades legales, en especial las conferidas por los artículos 19 y 21 de la Ley 1581 de 2012 y el numeral 8 del artículo 16 del Decreto 4886 de 2011 (modificado por el Decreto 092 de 2022), y

CONSIDERANDO:

PRIMERO. Que la Dirección de Investigación de Protección de Datos Personales, mediante Resolución No. 63771 del 15 de septiembre de 2022, respecto de la actuación administrativa adelantada en contra de **DATASET TECNOLOGIES S.A.S. EN LIQUIDACION** (en adelante **DATASET**) resolvió lo siguiente:

> ***"ARTÍCULO PRIMERO: IMPONER*** *la sanción a la sociedad comercial* ***DATASET TECNOLOGIES S.A.S. - EN LIQUIDACIÓN-*** *con NIT.: 900.520.797-7, la suspensión de actividades que involucren el Tratamiento de datos personales mediante su portal www.datajuridica.com, hasta por el término de (6) seis meses, contados a partir de la ejecutoria del presente acto administrativo, por la violación de lo previsto en el literal (o) del artículo 17 de la Ley 1581 de 2012, en concordancia con el artículo 19 de la misma ley, en tanto se acredite el cumplimiento de las siguientes instrucciones:*
>
> *(1) Establecer una metodología por medio de la cual se obtenga el consentimiento expreso, previo e informado de los titulares para que su información pueda ser consultada a través del portal www.datajuridica.com.*
>
> *(2) Abstenerse de utilizar tecnologías automatizadas, incluyendo, pero no limitándose, a robots, crawlers informáticos y similares para consultar información de los titulares de las páginas de consulta de procesos de la Rama Judicial; debiendo reemplazarla por una metodología de consulta a demanda para el titular en particular de forma posterior a la obtención de su autorización en los términos establecidos por el Régimen de Protección de Datos.*
>
> *(3) Dar cumplimiento a las Políticas de Tratamiento de la Información de la Rama Judicial, en es especial la prohibición de hacer uso comercial de la información personal reportada en los portales de consulta de procesos de la Rama Judicial.*
>
> *(4) Tomar medidas de mejoras frente a la tecnología implementada para la recolección de la información, teniendo en cuenta el principio de veracidad, incluyendo que la información arrojada al usuario final y la prohibición por parte de la Rama Judicial en relación con la prohibición de la sustracción sistematizada de la información contenida en sus páginas de consulta.*
>
> *(5) Garantizar, para cualquier tipo de consulta, que la información que se entregue al usuario final sobre cualquier titular, previa la otorgación de su autorización, sea actualizada, veraz, completa, y no induzca a error al usuario con respecto a su temporalidad;*
>
> *(6) Eliminar todos los datos personales, de cualquier naturaleza, hayan podido adquirirse de las páginas de consulta de la Rama Judicial por no haber obtenido la autorización en los términos establecidos por la L.1581/12.*
>
> *(7) Establecer los mecanismos necesarios y automatizados para que la investigada, previo al Tratamiento de los datos, obtenga el consentimiento de los titulares.*
>
> *(8) Implementar dentro de las de las Políticas de Protección de la Información una descripción expresa de la finalidad el Tratamiento que se pretende dentro de portal de la investigada".*

SEGUNDO. Lo anterior, en la medida que la Dirección consideró, conforme a las pruebas allegadas a la presente actuación, que **DATASET** vulneró las normas contenidas en la Ley 1581 de 2012, respecto del Tratamiento de la información a través del sitio web www.datajuridica.com

TERCERO. Que **DATASET** a través de su apoderado especial (en adelante el **RECURRENTE**), interpuso recurso de reposición y en subsidio apelación[1] contra la Resolución No. 63771 del 15 de septiembre de 2022, cuyos argumentos son los señalados en el escrito obrante en el consecutivo 75 del radicado No. 18-153189 del 10 de octubre de 2022.

CUARTO. Que mediante Resolución No. 417 del 16 de enero de 2023, la Dirección de Investigación de Protección de Datos Personales, resolvió el recurso de reposición interpuesto, confirmando en todas sus partes la Resolución No. 63771 del 15 de septiembre de 2022.

QUINTO. Que de conformidad con lo establecido en el artículo 80 del Código de Procedimiento Administrativo y de lo Contencioso Administrativo, este despacho confirmará el acto administrativo recurrido de acuerdo con lo que pasa a exponerse:

1. **Cuando un Responsable o Encargado del Tratamiento realiza "Scrapeo", o "*web scraping*", debe hacerlo en cumplimiento de lo establecido por el Régimen General de Protección de Datos Personales.**

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[2] 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.

Los Responsables del Tratamiento que realizan este tipo de prácticas, Tratamiento a gran escala[3], aprovechan la información para diversos fines, como su monetización mediante su reutilización en sitios web de terceros, su venta a actores maliciosos o su análisis privado. Algunas de las preocupaciones que presenta para el debido Tratamiento de Datos Personales, este tipo de prácticas, son las siguientes:

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.

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[4].

---

[1] La Resolución No. 54056 del 12 de agosto de 2022 fue notificada por aviso a DATASET el 27 de septiembre de 2022.
[2] Declaración conjunta de Autoridades de Protección de Datos Personales sobre el Web Scrapping: https://ico.org.uk/media/about-the-ico/documents/4026232/joint-statement-data-scraping-202308.pdf
[3] El Tratamiento de datos a gran escala es aquel que afecta a una gran cantidad de datos, referentes a un elevado número de Titulares, procedentes de una amplia diversidad geográfica, y que pueden entrañar un riesgo para los interesados.
[4] 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.

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.

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 "*bots*[5]". 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 Delegatura para la Protección de Datos Personales 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.

En conclusión, los Responsables y Encargados del Tratamiento que extraen, por mecanismos automatizados y/o análogos, información personal, están obligados a garantizar los postulados del Régimen General de Protección de Datos Personales.

2. De la calidad de Responsable de la Información por parte de DATASET. Su estado de Liquidación no lo exime del Cumplimiento de las normas de Protección de Datos Personales.

Indica el **RECURRENTE** en su escrito que, *"[c]omo fundamento principal de todos los cargos presentados por parte de esa Superintendencia para la interposición de la sanción establecida en la resolución bajo estudio, indica esa Entidad que DATASET es el responsable de la operación jurídica de DATAJURIDICA".*

Pues bien, el artículo 3 de la Ley 1581 de 2012, define entre otros términos aplicables al régimen de protección de datos personales, los siguientes:

> *"(…)*
>
> *b) Bases de Datos: Conjunto organizado de datos personales que sea objeto de Tratamiento;*

[5] Programa informático que realiza tareas automatizadas específicas y, generalmente, repetitivas en una red.

> *c) Dato Personal: Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables;*
>
> *(…)*
>
> *e) Responsable del Tratamiento: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de datos;*
>
> *(…)*
>
> *g) Tratamiento: Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión."*

Conforme a las citadas definiciones, el Responsable del Tratamiento realiza dos (2) actividades en materia de datos, la primera relacionada con la decisión sobre bases de datos, y la segunda, que refiere al Tratamiento de datos, actividades que no dependen una de la otra, en la medida que un Responsable puede realizar Tratamiento de información sin que se suponga la existencia de una base datos.

Frente este asunto en particular, este Despacho en la Resolución No. 54265 del 11 de octubre de 2019[6], indicó:

> *"En otras palabras, el Tratamiento de datos no supone la existencia de una base de datos. De hecho, puede existir Tratamiento sin que exista base de datos. Piénsese, por ejemplo, cuando alguien recolecta datos mediante páginas web, "cookies" [19][7] u otros mecanismos a través de internet. La simple recolección es un Tratamiento sin que sea necesario almacenar o usar el dato recolectado.*
>
> *Como se mencionó, el término "Tratamiento" se refiere a "cualquier operación o conjunto de operaciones sobre datos personales tales como la recolección, almacenamiento, uso, circulación o supresión" [20][8]. Esta expresión es de uso "técnico en el ámbito de los datos personales. Y es de gran importancia porque ha sido incluida en el artículo 15 de nuestra Constitución Política cuando ordena que, "En la recolección, **Tratamiento** y circulación de datos se respetará la libertad y demás garantías consagradas en la Constitución".*

La Corte Constitucional respecto del término Tratamiento, en el numeral 2.5.9 de la Sentencia C – 748 de 2011, precisó lo siguiente:

> *"(…) cuando el proyecto se refiere al **Tratamiento,** hace alusión a cualquier operación que se pretenda hacer con e dato personal, con o sin ayuda de la informática, pues a diferencia de algunas legislaciones, la definición que así se analiza no se circunscribe únicamente a procedimientos automatizados. Es por ello que principios, derechos, deberes y sanciones que contempla la normativa en revisión incluyen, entre otros, la recolección, la conservación, la utilización y otras formas de procesamiento de datos con o sin ayuda de la informática. En consecuencia, no es válido argumentar que la ley de protección de datos personales cobija exclusivamente el Tratamiento de datos que emplean las nuevas tecnologías de la información, dejando por fuera las bases de datos manuales, lo que resultaría ilógico, puesto que precisamente **lo que se pretende con este proyecto es que todas las operaciones o conjunto de operaciones con los datos personales quede regulada por las disposiciones del proyecto de ley en mención,** con las salvedades que serán analizadas en otro apartado de esta providencia. En este orden de ideas, esta definición no genera problema alguno de constitucionalidad y por tanto será declarada exequible". (Negrita fuera de texto).*

Así las cosas, la calidad de Responsable no se limita únicamente al manejo de bases de datos, sino también al Tratamiento que realice de la información de acuerdo con sus actividades.

En el caso particular, informó **DATASET** a través del oficio No. 18-153189-09 del 14 de septiembre de 2018, que, *"Los resultados de las búsquedas no se encuentran almacenados en bases de datos de nuestra propiedad pues no hay necesidad. **Cada vez que el usuario realiza una consulta, data jurídica realiza la búsqueda directamente a las fuentes mencionadas On line de donde arma la lista de resultados**".*

La descripción anterior, encaja en la definición de Tratamiento, teniendo en cuenta que, la información es tratada para que el resultado de la búsqueda que se realiza en las diferentes fuentes mencionadas esté al alcance de quien se suscribe y realiza el pago para obtener el servicio ofertado

---

[6] Decisión expedida dentro del radicado No. 17-298068

[7] Mediante concepto Radicado No. 16-172268 del 9 de agosto de 2016 la Oficina Jurídica de la SIC concluyó que "Las cookies son archivos que recogen información a través de una página web sobre los hábitos de navegación de un usuario o de su equipo y eventualmente podrían conformar una base de datos de acuerdo ca la definición legal de la Ley 1581 de 2012 al recolectar datos personales." El texto completo del concepto se puede consultar en: https://www.sic.gov.co/recursosuser/boletin-juridico-sep2016/conceptos/datos_personales/16172268-proteccion-datos-9-ago-2016.pdf

[8] [20] Literal g) del artículo 3 de la Ley 1581 de 2012

por www.datajuridica.com, información que, en algunos de los casos reportados ante esta Superintendencia, no es veraz o actualizada.

Ahora bien, afirma el **RECURRENTE** que, *"[c]on todo lo dicho queda demostrado que DATASET no puede fungir como responsable de la página DATAJURIDICA y esa sola consideración bastaría para que la resolución sancionatoria impuesta carezca de sentido, en la medida que, como se entra además a dilucidar le queda imposible dar cumplimiento a la orden impartida al no tener ningún tipo de potestad para poderla llevar a cabo".*

En este punto en particular, debe recordársele al **RECURRENTE**, que una cosa es ser el propietario del dominio de una página web y otra, el Responsable del Tratamiento de la información, y es precisamente esta responsabilidad la que se le endilga a **DATASET** en la presente actuación administrativa, pues definió en conjunto con **PROXY SYSTEMS,** bajo el régimen de protección de datos personales, el Tratamiento de la información de los titulares que tuvieron acceso al motor de búsqueda ofrecido desde el sitio web www.datajuridica.com.

Finalmente, para este Despacho es de suma importancia dejar claridad sobre lo siguiente. La personalidad jurídica de las sociedades se extingue con la inscripción de la cuenta final de la liquidación. **Estar en proceso de liquidación no exime a la sociedad recurrente de sus deberes como Responsable del Tratamiento de esa información**. Por eso, las entidades públicas y privadas, así se encuentren en proceso de liquidación, deben ser muy responsables, diligentes y muy profesionales con el Tratamiento adecuado de dichos datos.

Aunque la sociedad recurrente se encuentre en liquidación, el almacenamiento y la supresión de los datos forman parte del Tratamiento de Datos Personales. Los correctivos impartidos por esta Superintendencia se encuentran encaminados a que **DATASET** realice un debido Tratamiento de los datos, toda vez que esta, en su calidad de Responsable del Tratamiento, debe cumplir con las disposiciones de ley.

Así, el Responsable del Tratamiento no es solo aquel que recolecta los datos, sino quien los almacena en un momento determinado. Es decir que si dicha sociedad guardó o archivó datos o bien suprime los mismos de sus bases de datos, debe hacerlo con todas las medidas de seguridad para garantizar el debido Tratamiento de estos y no poner en riesgo los derechos de las personas.

De esta manera, si bien la sociedad se encuentre en liquidación, recuerda el Despacho que esto no la exime de dar estricto cumplimiento a la regulación sobre Tratamiento de datos personales y a las órdenes emitidas por esta Superintendencia por cuanto mientras trate esa información, dicho Tratamiento debe ser realizado conforme a la ley.

3. Frente a la vulneración del principio de acceso y circulación restringida. No todo dato de acceso público es, per se, de naturaleza pública. La naturaleza jurídica de un dato público no depende únicamente de que su acceso sea libre.

Indica el **RECURRENTE** que, "*esta Superintendencia reprocha a DATASET que a través del portal DATAJRIDICA puedan encontrarse datos, que como se menciono son datos básicos de los procesos que se tienen en la rama judicial y son publicados por esta para consulta pública*".

Sostiene igualmente que, *"si este es el argumento de la Superintendencia, me permito recordar que las actuaciones de los administrados de basan en l seguridad jurídica que los administradores dan sobre sus actuaciones, de manera que de sostenerse esta teoría que al parecer nace con esta resolución. El administrado tendría en adelante que dudar de toda información que hagan sus autoridades y en cuando a la posibilidad de consultar su información".*

El artículo 4 literal f) de la Ley 1581 de 2012, establece lo siguiente:

> *f) Principio de acceso y circulación restringida: El Tratamiento se sujeta a los límites que se derivan de la naturaleza de los datos personales, de las disposiciones de la presente ley y la Constitución. En este sentido, el Tratamiento sólo podrá hacerse por personas autorizadas por el Titular y/o por las personas previstas en la presente ley;*
>
> *Los datos personales, salvo la información pública, no podrán estar disponibles en Internet u otros medios de divulgación o comunicación masiva, salvo que el acceso sea técnicamente controlable para brindar un conocimiento restringido sólo a los Titulares o terceros autorizados conforme a la presente ley;*

La Corte Constitucional cuando revisó la constitucional de la citada Ley, respecto del principio de acceso y circulación restringida, manifestó lo siguiente:

> ***"Principio de acceso y circulación restringida:*** *En razón de esta directriz, el Tratamiento se sujeta a los límites que se derivan de la naturaleza de los datos personales, de las disposiciones de la presente ley y la Constitución. En este sentido, éste sólo podrá hacerse por personas autorizadas por el titular y/o por las personas previstas en la presente ley. Además, se prohíbe que los datos personales, salvo información pública, se encuentren disponibles en Internet, a menos que se ofrezca un control técnico para asegurar el conocimiento restringido.*
>
> *En relación con* ***el primer inciso****, deben hacerse las siguientes precisiones. Como se explicó anteriormente, esta Ley Estatutaria, al establecer las condiciones mínimas en el manejo de la información, no agota la regulación en materia de habeas data, y por tanto, el Tratamiento estará también sujeto a la normatividad que se expida posteriormente.*
>
> *En cuanto* ***al segundo inciso****, la norma debe entenderse que también se encuentra prohibida toda conducta tendiente al cruce de datos entre las diferentes bases de información, excepto cuando exista una autorización legal expresa, es decir, lo que la jurisprudencia ha denominado el* ***principio de individualidad*** *del dato. Como consecuencia de lo anterior, queda prohibido generar efectos jurídicos adversos frente a los Titulares, con base,* ***únicamente*** *en la información contenida en una base de datos.*
>
> *De otra parte, y en relación con ese segundo inciso, uno de los interviniente solicita a esta Corporación, declarar su constitucionalidad bajo los siguientes condicionamientos:* ***(i) se debe evitar que los datos privados, semiprivados, reservados o secretos puedan estar junto con los datos públicos****, y por tanto,* ***los primeros no pueden ser objeto de publicación en línea, a menos que se ofrezcan todos los requerimientos técnicos*** *y* ***(ii) se debe eliminar cualquier posibilidad de acceso indiscriminado, mediante la digitación del número de identificación a los datos personales del ciudadano****. (Destacamos)*
>
> *Considera la Sala que tales condicionamientos no son necesarios, por cuanto la misma norma elimina estas posibilidades. En efecto:* ***(i)*** *prohíbe que los datos no públicos sean publicados en Internet y* ***(ii)*** *sólo podrían ser publicados si se ofrecen todas las garantías. De lo anterior se infiere que si el sistema permite el acceso con la simple digitación de la cédula, no es un sistema que cumpla con los requerimientos del inciso segundo del literal f) del artículo 4.*
>
> *Sin embargo, 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.*
>
> *De otra parte, cabe señalar que aún cuando se trate de información pública, su divulgación y circulación está sometida a los límites específicos determinados por el objeto y finalidad de la base de datos."*

Conforme lo anterior, los Responsables al realizar el Tratamiento de la información de los titulares, debe evitar que los datos privados, semiprivados inclusive sensibles, puedan estar junto a aquellos datos de naturaleza pública, pues, de no ser así, el Responsable deberá garantizar que su Tratamiento esté supeditado a la autorización del titular del dato.

Ahora bien, el numeral segundo del artículo 2.2.2.25.1.3 del Decreto 1074 de 2015, define el Dato público en los siguientes términos:

> *"2. Dato público. Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva.*

En este punto resulta necesario precisar que, **el hecho de que un dato personal sea de acceso público NO significa que, por esa sola razón sea un dato de naturaleza pública**. Al respecto, el inciso segundo del artículo 2.2.2.25.2.2 del Decreto 1074 de 2015, señala lo siguiente:

> *"Los datos personales que se encuentren en fuentes de acceso público, con independencia del medio por el cuál se tenga acceso, entendiéndose por tales aquellos datos o bases de datos que se encuentren a disposición del público, pueden ser tratados por cualquier* ***persona siempre y cuando, por su naturaleza, sean datos públicos****".*

Conforme lo anterior, no todo dato de acceso público es, *per se*, de naturaleza pública. La naturaleza jurídica de un dato público no depende únicamente de que su acceso sea libre. De ser así, equivocadamente se concluiría que todos los datos personales que reposan en internet son de naturaleza púbica y por ende cualquier persona puede tratarlos sin autorización previa, expresa e informada del Titular del Dato.

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 usa "innovaciones tecnológicas" deben cumplir todas las normas de protección de datos.

4. La información de un titular que se reúna a través de un motor de búsqueda, debe cumplir con las exigencias del principio de veracidad.

Afirmó el **RECURRENTE**, que, *"si alguien recibe información de una página del estado, cualquiera que sea la rama de que se trate, lo primero que debe tenerse en consideración es que esa persona, sea natural o jurídica parte de la buena fe de las actuaciones, así como de la capacidad del organismo estatal que la presenta para su consulta de entregarla de forma veraz y actualizada".*

El artículo 20 de la Constitución Política, consagra el derecho de informar y recibir información "veraz e imparcial". Estas calidades constitucionales también deben atribuirse de los datos personales. Así, quien suministre o trate datos, debe asegurarse de la veracidad y exactitud de los mismos. En este sentido, la Corte Constitucional ha señalado que, "los datos personales deben obedece a situaciones reales, deben ser ciertos, de tal forma que se encuentra prohibida la administración de datos falsos o erróneos"[9]. En otras palabras, de la citada corporación, el principio de veracidad exige que *"los datos personales deben corresponder a situaciones reales, lo que impone la prohibición de recopilar, procesar y circular información falsa, errónea o equívoca"*[10].

Por su parte, el literal d) del artículo 4 de la Ley 1581 de 2012, define el principio de veracidad, en los siguientes términos:

> *"d) Principio de veracidad o calidad: La información sujeta a Tratamiento debe ser veraz, completa, exacta, actualizada, comprobable y comprensible. Se prohíbe el Tratamiento de datos parciales, incompletos, fraccionados o que induzcan a error;*

La veracidad de los datos **es una exigencia mínima para que los sistemas de información sean confiables, y sobre todo para que no se afecten los derechos de las personas**. No es útil para la sociedad acceder a información que no sea veraz ni de calidad. Así resultaría impropio e insistente con los postulados constitucionales, circular datos erróneos, incompletos, inexactos, desactualizados o falsos sobre las personas.

Así las cosas, en desarrollo del principio veracidad, **la información de un titular que se reúna a través de un motor de búsqueda, debe cumplir con las exigencias del principio de veracidad**, por lo que el Responsable debe abstenerse de circular datos falsos que puedan inducir en error a aquellas personas que los consultan.

5. Los Responsables del Tratamiento deben obtener la autorización para el Tratamiento de Datos Personales de naturaleza sensible, privada y semiprivada.

El artículo 15 de la Constitución Política, establece que *"[t]odas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho 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*".

Dicha norma establece que las personas, en desarrollo de sus derechos a la autodeterminación informática y el principio de libertad, son quienes de forma expresa deben autorizar que la información que sobre ellos sea recaudada pueda ser incluida en una base de datos.

En desarrollo de lo anterior, el literal b) del artículo 17 la Ley 1581 de 2012 le impone a los Responsables del Tratamiento de Datos Personales el deber de ***"[s]olicitar y conservar, en las condiciones previstas en la presente ley, copia de la respectiva autorización otorgada por el Titular"****;*

---

[9] Corte Constitucional, T-729 de 2002.
[10] Corte Constitucional, C-1011 de 2008.

Respecto de la autorización para el Tratamiento de datos personales, el artículo 9 de la mencionada Ley, dispone:

> ***ARTÍCULO 9o. AUTORIZACIÓN DEL TITULAR.*** *Sin perjuicio de las excepciones previstas en la ley,* ***en el Tratamiento se requiere la autorización previa e informada del Titular****, la cual deberá ser obtenida por cualquier medio que pueda ser objeto de consulta posterior.*

El Decreto 1074 de 2015, a través de los artículos 2.2.2.25.2.4 y 2.2.2.25.2.5 en lo que tiene que ver con el modo de obtener la autorización y su prueba, dispone lo siguiente:

> ***"Artículo 2.2.2.25.2.4. Modo de obtener la autorización.*** *Para efectos de dar cumplimiento a lo dispuesto en el artículo 9 de la Ley 1581 de 2012, los Responsables del Tratamiento de datos personales establecerán mecanismos para obtener la autorización de los titulares o de quien se encuentre legitimado de conformidad con lo establecido en el artículo 2.2.2.25.2.1, del presente Decreto, que garanticen su consulta. Estos mecanismos podrán ser predeterminados a través de medios técnicos que faciliten al Titular su manifestación automatizada.*
>
> *Se entenderá que la autorización cumple con estos requisitos cuando se manifieste (i) por escrito (ii) de forma oral o (iii) mediante conductas inequívocas del titular que permitan concluir de forma razonable que otorgó la autorización. En ningún caso el silencio podrá asimilarse a una conducta inequívoca.*
>
> ***Artículo 2.2.2.25.2.1 Prueba de la autorización.*** *Los Responsables deberán conservar prueba de la autorización otorgada por los titulares de datos personales para el Tratamiento de los mismos".*

Por su parte el artículo 10 de la Ley 1581 de 2012, dispone lo siguiente:

> *"****ARTÍCULO 10. CASOS EN QUE NO ES NECESARIA LA AUTORIZACIÓN****. La autorización del Titular no será necesaria cuando se trate de:*
> *a) Información requerida por una entidad pública o administrativa en ejercicio de sus funciones legales o por orden judicial;*
> ***b) Datos de naturaleza pública;***
> *c) Casos de urgencia médica o sanitaria;*
> *d) Tratamiento de información autorizado por la ley para fines históricos, estadísticos o científicos;*
> *e) Datos relacionados con el Registro Civil de las Personas.*
> *Quien acceda a los datos personales sin que medie autorización previa deberá en todo caso cumplir con las disposiciones contenidas en la presente ley".*

De conformidad con las normas anteriormente citadas, el Responsable del Tratamiento debe solicitar al titular la respectiva autorización, esto, para informarle que, sus datos personales serán tratados conforme a las normas legales; dicha autorización debe ser solicitada en todos los casos excepto aquellos que estén relacionados en el ya citado artículo 10 de la Ley 1581 de 2012.

Pues bien, de acuerdo con las quejas presentadas ante esta Superintendencia, parte de la información tratada por parte de **DATASET**, no sólo son datos de naturaleza pública, sino aquellos de índole privado, semiprivado e inclusive sensibles. **Situación que lleva a concluir al Despacho que el motor de búsqueda desarrollado para el portal web de datajuridica no consideró el principio de privacidad desde el diseño y por defecto[11], toda vez que ésta se encuentra diseñada para la visualización de todo tipo de datos personal sin importar su naturaleza**.

Luego entonces, para que no tenga que realizar las actividades tendientes a obtener de los titulares la autorización para el Tratamiento de su información, deberá asegurarse que la información que vaya a ser tratada únicamente se trate de aquella de naturaleza pública.

6. Caducidad de la Facultad Sancionatoria. En el presente caso, esta Superintendencia contaba hasta el 31 de diciembre de 2022 para imponer la sanción correspondiente

El artículo 52 del Código de Procedimiento Administrativo y de lo Contencioso Administrativo, establece:

> *"ARTÍCULO 52. CADUCIDAD DE LA FACULTAD SANCIONATORIA. Salvo lo dispuesto en leyes especiales,* ***la facultad que tienen las autoridades para imponer sanciones caduca a los tres (3) años de ocurrido el hecho, la conducta u omisión que pudiere ocasionarlas, término dentro del cual el acto administrativo que impone la sanción debe haber sido expedido y notificado****. (…)*
>
> ***Cuando se trate de un hecho o conducta continuada, este término se contará desde el día siguiente a***

[11] La privacidad desde el diseño y por defecto (Privacy by Design and by Default) es considerada una medida proactiva para cumplir con el Principio de Responsabilidad Demostrada.

***aquel en que cesó la infracción y/o la ejecución**". (Destacamos).*

Respecto de la Facultad sancionatoria de la administración, el Consejo de Estado[12] manifestó lo siguiente:

> *3.4.2. En un reciente pronunciamiento, la Sección Primera del Consejo de Estado, mediante sentencia del 12 de diciembre de 2019[13], también mantuvo la anterior postura. En esa oportunidad, la Sección Primera del Consejo de Estado analizó la legalidad de actos administrativos sancionatorios y sostuvo que aunque la sentencia del 29 de septiembre de 2009 versó sobre una sanción de carácter disciplinario, esa Sección había determinado de manera reiterada que las consideraciones ahí expuestas eran plenamente aplicables a aquellas controversias que se rigen por el artículo 38 del CCA. De manera que "en el término previsto para ejercer la facultad sancionatoria, las autoridades administrativas deben expedir y notificar el acto administrativo principal sancionatorio, sin que estén sometidas a que dentro de ese mismo plazo deban resolver los eventuales recursos que se interpongan contra dicha decisión; **en ese orden de ideas, la administración únicamente pierde competencia para imponer sanciones, cuando trascurrido el término de tres años, no ha expedido y notificado el respectivo acto administrativo sancionatorio**" (subraya la Sala). (Negrilla del Despacho).*

Quiere decir entonces que la facultad sancionatoria de la administración no puede perpetuarse en el tiempo, hacerlo constituye una clara vulneración del debido proceso, que va en contravía del principio de seguridad jurídica que debe regir en las actuaciones administrativas.

El artículo 52 del CPACA antes citado, establece dos escenarios que deben a tenerse en cuenta para la contabilización del término de 3 años, el primero, se cuenta a partir de la fecha en que ocurrió el hecho como una conducta instantánea, y el segundo, cuando se trata una conducta continuada en el tiempo**, evento en el cual el término de caducidad se empezará a contar desde el día siguiente a que haya cesado la vulneración de la norma**.

Al respecto el Consejo de Estado[14] señaló que:

> *"Las conductas instantáneas se agotan en un solo momento**,** en tanto que las de ejecución sucesiva se prolongan en el tiempo, lo que significa que la comisión de la conducta objeto de investigación tiene el carácter de permanente o continuada, de tal suerte que la facultad sancionatoria de la administración debe computarse a partir de la comisión o realización del último acto de ejecución.*
>
> *En efecto, **en el evento de investigarse una conducta permanente o continuada, el Consejo de Estado ha sostenido que el término de caducidad para imponer la sanción[15] "comienza a contarse a partir de la fecha en la cual cesa dicha conducta**. De allí que en los demás casos, dicho plazo se contabilizará en la forma establecida por el artículo 38 del C.C.A., esto es, desde que el hecho se produce"[16].*

Conforme lo anterior, cuando se revisan los hechos que dieron origen a la presente actuación administrativa, evidencia el Despacho que estamos frente a una conducta continuada en el tiempo, en la medida que la vulneración a las normas de protección de datos personales, entiende el Despacho, cesó el 31 de diciembre de 2019, fecha en la cual **DATASET** entró en proceso de liquidación.

Como consecuencia, en el presente caso, esta Superintendencia contaba hasta el 31 de diciembre de 2022 para imponer la sanción correspondiente, situación que se dio, pues el acto administrativo que se revisa, fue expedido el 15 de septiembre de 2022, así las cosas, en el presente caso no se configura el fenómeno de la caducidad, descrto en el a citado artículo 52 del CPACA.

---

[12] C.E., Sec. Cuarta, Sent. 11000103150002020030350O, ago. 20/2020 C.P. Julio Roberto Piza Rodríguez.
[13] M.P. Hernando Sánchez Sánchez. Expediente 2006-00115-01.
[14] Consejo de Estado, Sección Sección Primera, en sentencia de 22 de mayo de 2014 (Expediente núm. AC-2013-02392-00, M.P. Marco Antonio Velilla Moreno "Dado lo anterior, quedó demostrado que esta Corporación ha realizado un análisis sobre el término de la caducidad de la facultad sancionatoria concerniente a hechos distintos, como las infracciones en materia de energía que fueron en forma continuada donde la ocurrencia del hecho se contó a partir del último acto, o en el caso aduanero que a pesar de tener norma especial que regula el tema, se parte que existe conocimiento de la falta desde que la entidad inicie el trámite administrativo…".
[15] Consejo de Estado, Sección Quinta, Sentencia del 12 de abril de 2018, M.P. Carlos Enrique Moreno Rubio, Radicación número: 25000-23-24-000-2012-00788-01, actor: ALIANSALUD ENTIDAD PROMOTORA DE SALUD S. A.
[16] Consejo de Estado, Sección Primera, Sentencia del 18 de agosto de 2011, M.P. Rafael E. Ostau de Lafont Pianeta, Radicación número: 11001-03-24-000-2007-00013-00, posición reiterada en providencia del 8 de febrero de 2018, exp. 25000-23-24-000-2008-00045-02, M.P. Rocío Araújo Oñate, actor: Empresa de Acueducto y Alcantarillado de Bogotá (EAAB).

7. Precisión Final.

Este Despacho, al verificar nuevamente la Resolución No. 63771 del 15 de septiembre de 2022, advierte un error de orden formal en su parte resolucitva, que, si bien no afecta en modo alguno el sentido de la decisión tomada por parte de la Dirección de Investigación de Protección de Datos Personales, este Despacho procederá a modificarla de conformiad con lo establecido en el artículo 45 del Código de Procedimiento Administrativo y de lo Contencioso Administrativo.

Finalmente, este Despacho considera necesario modificar las instrucciones dadas por la Dirección de Investigación de Protección de Datos Personales en el acto administrativo que se revisa, esto con el fin de que las mismas sean efectivamente acogidas por parte de **DATASET**.

8. Conclusiones.

- Cuando un Responsable o Encargado del Tratamiento realiza “Scrapeo”, o “web scraping”, debe hacerlo en cumplimiento de lo establecido por el Régimen General de Protección de Datos Personales.
- Los Titulares pierden el control cuando su información personal se extrae sin su conocimiento y en contra de sus expectativas.
- La calidad de Responsable no se limita únicamente al manejo de bases de datos, sino también al Tratamiento que realice de la información de acuerdo con sus actividades.
- Estar en proceso de liquidación no exime a la sociedad recurrente de sus deberes como Responsable del Tratamiento de esa información. Por eso, las entidades públicas y privadas, así se encuentren en proceso de liquidación, deben ser muy responsables, diligentes y muy profesionales con el Tratamiento adecuado de dichos datos.
- El hecho de que un dato personal sea de acceso público NO significa que, por esa sola razón sea un dato de naturaleza pública.
- El propietario del dominio de una página web no siempre es el Responsable del Tratamiento de la información. DATASET en conjunto con PROXY SYSTEMS, definió bajo el régimen de protección de datos personales el Tratamiento de la información de los titulares que tuvieron acceso al motor de búsqueda ofrecido desde el sitio web www.datajuridica.com.
- El Responsable del Tratamiento debe solicitar al Titular la respectiva autorización, esto, para informarle que, sus datos personales serán tratados conforme a las normas legales; dicha autorización debe ser solicitada en todos los casos excepto aquellos que estén relacionados en el ya citado artículo 10 de la Ley 1581 de 2012.
- En desarrollo del principio veracidad antes desarrollado, **la información de un titular que se reúna a través de un motor de búsqueda, debe cumplir con las exigencias del principio de veracidad**, por lo que el Responsable debe abstenerse de circular datos falsos que puedan inducir en error a aquellas personas que los consultan.
- No es útil para la sociedad acceder a información que no sea veraz ni de calidad.
- Conforme a lo desarrollado por parte de la Dirección de Investigación de Protección de Datos Personales, frente a las quejas presentadas por diferentes usuarios de la página web www.dtajuridica.com, considera el Despacho que el motor de búsqueda desarrollado para dicho portal no consideró el principio de privacidad desde el diseño y por defecto, toda vez que el que se encontraba en uso, no estaba diseñado para la visualización de datos únicamente de naturaleza pública.
- En el presente caso, la Dirección de Investigación de Protección de Datos Personales impuso la sanción dentro del término establecido de 3 años establecido en el artículo 52 del Código de Procedimiento Administrativo y de lo Contencioso Administrativo.
- 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 usa “innovaciones tecnológicas” deben cumplir todas las normas de protección de datos.
- Este Despacho concluye que el motor de búsqueda desarrollado para el portal web de datajuridica no consideró el principio de privacidad desde el diseño y por defecto, toda vez que ésta se encuentra diseñada para la visualización de todo tipo de datos personal sin importar su naturaleza.

De esta forma y de acuerdo con lo dispuesto por el artículo 80 del Código de Procedimiento Administrativo y de lo Contencioso Administrativo, este Despacho confirmará la Resolución No. 63771 del 15 de septiembre de 2022.

En mérito de lo expuesto, este Despacho

RESUELVE:

ARTÍCULO 1. MODIFICAR el **ARTÍCULO PRIMERO** de la Resolución No. 63771 del 15 de septiembre de 2022, de conformidad con lo expuesto en la parte motiva de la presente resolución, el cual quedará así:

> ***"ARTÍCULO PRIMERO: IMPONER*** *la sanción a la sociedad comercial* ***DATASET TECNOLOGIES S.A.S. - EN LIQUIDACIÓN-*** *con NIT.: 900.520.797-7, la suspensión de actividades que involucren el Tratamiento de datos personales mediante su portal www.datajuridica.com, hasta por el término de (6) seis meses, contados a partir de la ejecutoria del presente acto administrativo, por la vulneración de los principios de acceso y circulación restringida de la información, veracidad y libertad, establecidos y desarrollados por la Ley 1581 de 2012, en tanto se acredite el cumplimiento de las siguientes instrucciones:*
>
> *(1) Establecer una metodología por medio de la cual se obtenga el consentimiento expreso, previo e informado de los titulares para que su información de naturaleza sensible, privada y/o semiprivada pueda ser consultada a través del portal www.datajuridica.com.*
>
> *(2) Abstenerse de utilizar tecnologías automatizadas, incluyendo, pero no limitándose, a robots, crawlers informáticos y similares para consultar información de los titulares de las páginas de consulta de procesos de la Rama Judicial; debiendo reemplazarla por una metodología de consulta a demanda para el titular en particular de forma posterior a la obtención de su autorización en los términos establecidos por el Régimen de Protección de Datos.*
>
> *(3) Dar cumplimiento a las Políticas de Tratamiento de la Información de la Rama Judicial, en especial la prohibición de hacer uso comercial de la información personal reportada en los portales de consulta de procesos de la Rama Judicial.*
>
> *(4) Tomar medidas de mejoras frente a la tecnología implementada para la recolección de la información, teniendo en cuenta el principio de veracidad, incluyendo que la información arrojada al usuario final y la prohibición por parte de la Rama Judicial en relación con la prohibición de la sustracción sistematizada de la información contenida en sus páginas de consulta.*
>
> *(5) Garantizar, para cualquier tipo de consulta, que la información de naturaleza sensible, privada y/o semiprivada que se entregue al usuario final sobre cualquier Titular, previa la otorgación de su autorización, sea actualizada, veraz, completa, y no induzca a error al usuario con respecto a su temporalidad;*
>
> *(6) Eliminar todos los datos personales, de naturaleza sensible, privada y/o semiprivada, que hayan podido adquirirse de las páginas de consulta de la Rama Judicial por no haber obtenido la autorización en los términos establecidos por la L.1581/12.*
>
> *(7) Establecer los mecanismos necesarios y automatizados para que la investigada, previo al Tratamiento de los datos de naturaleza sensible, privada y/o semiprivada, obtenga el consentimiento de los titulares.*
>
> *(8) Implementar dentro de las de las Políticas de Protección de la Información una descripción expresa de la finalidad el Tratamiento que se pretende dentro de portal de la investigada".*

ARTÍCULO 2. NOTIFICAR la presente decisión a la sociedad **DATASET TECNOLOGIES S.A.S. EN LIQUIDACION,** identificada con Nit. 900.520.797-7, a través de su representante legal y/o su apoderado, entregándole copia de la misma e informándole que contra el presente acto administrativo no procede recurso alguno.

ARTÍCULO 3. INFORMAR el contenido de la presente resolución al Director de Investigación de Protección de Datos Personales y devolverle el expediente para su custodia final.

NOTIFÍQUESE Y CÚMPLASE

Dada en Bogotá, D.C.,28 de septiembre 2023

EL SUPERINTENDENTE DELEGADO PARA LA PROTECCIÓN DE DATOS PERSONALES (E),

ALEJANDRO LONDOÑO CONGOTE

NTL

NOTIFICACIÓN:

Sociedad:	**DATASET TECNOLOGIES S.A.S. EN LIQUIDACIÓN**
Identificación:	Nit. 900.520.797-7
Representante legal:	**RODOLFO IGNACIO CORREAL GARCÍA**
Identificación:	C.C. 79.541.122
Dirección:	Calle 69 No. 4 – 12
Correo Electrónico:	rodocorreal@hotmail.com
Apoderado Especial:	**JOSE IGNACIO PEDRO ELIAS NOVOA SERRANO**
Identificación:	C.C. 79.592.192
Tarjeta Profesional:	100.709 del C.S. de la J
Dirección:	Carrera 19ª No. 84 – 29 Oficina 704
Correo electrónico:	pnovoa@mscol,co