TEMAS-SUBTEMAS

Sentencia T-067/25

DERECHO DE ACCESO A LA INFORMACIÓN PÚBLICA-Transparencia mediante suministro de código fuente de aplicación informática

(...) al no encontrarse acreditada la carga probatoria (artículo 28 de la Ley 1712 de 2014) respecto de la configuración del daño que justificaría las excepciones al acceso a la información pública solicitada por el actor, las autoridades accionadas violaron el derecho de acceso a la información pública. Adicionalmente, se afectó el ejercicio de otros derechos. En el caso específico, la falta de transparencia y acceso al código fuente de la aplicación CoronApp privó tanto al ciudadano accionante como a la sociedad en general de la posibilidad de ejercer un control adecuado y oportuno sobre esa herramienta. Esta deficiencia no solo disminuyó la extensión, obligatoriedad y funcionalidad del derecho fundamental al acceso a la información pública, sino que también impidió que los ciudadanos pudieran verificar la precisión, seguridad y uso correcto de sus datos personales, limitando así su capacidad para proteger sus derechos a la privacidad, a la protección de datos y a la participación informada en los procesos de toma de decisiones públicas.

DERECHO DE ACCESO A LA INFORMACIÓN PÚBLICA-Contenido y alcance

DERECHO DE ACCESO A LA INFORMACIÓN PÚBLICA-Instrumentos internacionales

DERECHO DE ACCESO A LA INFORMACIÓN PÚBLICA-Jurisprudencia constitucional

DERECHO DE ACCESO A LA INFORMACIÓN PÚBLICA-Reglas jurisprudenciales

DERECHO DE ACCESO A LA INFORMACIÓN PÚBLICA-Regulación normativa

DERECHO DE ACCESO A LA INFORMACIÓN-Test de daño al interés público/**RESTRICCION DE ACCESO A LA INFORMACION**-Motivación

El artículo 28 desarrolla lo que se conoce como el test del daño, que busca equilibrar el derecho de acceso a la información pública y la protección de ciertos intereses que se pueden ver afectados por la publicación de determinada información. Para ello, la norma establece que el sujeto obligado que niegue el acceso a determinada información pública alegando un daño a un interés particular o público debe demostrar que: a) la información está relacionada con un objetivo constitucional y legalmente legítimo; b) se trata de una de las excepciones expresamente establecidas en los artículos 18 y 19 de la Ley 1712 de 2014; c) la información causaría un daño presente, probable y específico sobre un bien o interés constitucional; d) dicho daño excede el interés público que representa el acceso a la información.

DERECHO AL HABEAS DATA-Alcance y contenido

DATOS PERSONALES-Características

DATOS SENSIBLES-Contenido

TRATAMIENTO DE DATOS PERSONALES-Contenido y alcance

DERECHO A LA INTIMIDAD-Alcance y contenido

SISTEMAS DE TOMA DE DECISIONES AUTOMATIZADAS (SDA)-Concepto y aspectos básicos acerca de su funcionamiento

DERECHO A LA INTIMIDAD EN SISTEMAS DE INTELIGENCIA ARTIFICIAL (IA)-Alcance de la privacidad en el manejo de información

TRANSPARENCIA ALGORÍTMICA-Garantía fundamental

(...) la transparencia en el uso de esta herramienta es una garantía fundamental para asegurar un empleo adecuado y razonable de los datos personales y evitar que el uso de sistemas algorítmicos para la toma de decisiones por parte de entidades públicas derive en decisiones arbitrarias o discriminatorias.

TRANSPARENCIA ALGORÍTMICA-Finalidad

Lo que se busca con la transparencia algorítmica es... que el público en general pueda comprender cómo los sistemas de toma de decisiones automatizadas (SDA) procesan los datos que capturan y cómo toman decisiones que afectan la vida de las personas. Se trata de un principio con un fin constitucional: democratizar el funcionamiento interno de un sistema de toma de decisión automatizado, para que sea entendible por quienes se ven afectados por su puesta en marcha y operación.

TRANSPARENCIA ALGORÍTMICA-Importancia

La transparencia algorítmica es particularmente relevante en el uso de SDA por parte de entidades públicas. Lo anterior, debido a que las decisiones que toma el Estado a través de estos sistemas tienen efectos importantes en materia de derechos.

DERECHO DE ACCESO A LA INFORMACIÓN PÚBLICA-Protección constitucional en el contexto de la pandemia COVID-19

DERECHO AL HABEAS DATA-Protección de su núcleo esencial en el contexto de la pandemia COVID-19

TRANSPARENCIA ALGORÍTMICA-Concepto

Se trata de una garantía fundamental en una sociedad democrática, pues si un sistema de toma de decisiones automatizadas (SDA) opera y toma decisiones de manera opaca, es imposible que la sociedad evalúe su capacidad de actuar con justicia y equidad, o su impacto en la autonomía y la dignidad de las personas. Como su propia definición lo revela, la transparencia algorítmica es un concepto que se deriva de un elemento que hace parte sustancial e inescindible de la naturaleza del derecho fundamental al acceso a la información pública: la disponibilidad de información.

SISTEMAS DE TOMA DE DECISIONES AUTOMATIZADAS (SDA)-Riesgos de la transparencia del código fuente

(...) aunque la publicación del código fuente es uno de los mecanismos a través de los cuales se puede garantizar la transparencia algorítmica, es claro

que presenta complejidades. Habrá situaciones en que una explicación significativa sobre el funcionamiento del sistema sea más apropiada que la publicidad total del código fuente, ya que esta puede crear riesgos desproporcionados para la seguridad nacional, o desconocer secretos empresariales. No obstante, es fundamental tener en cuenta que cuando se trata de SDA a cargo de entidades públicas, la transparencia algorítmica activa y pasiva debe guiarse bajo un principio de divulgación máxima. Según este principio, es fundamental que la información revelada al público para vigilar la acción digital del Estado permita examinar el desempeño de la aplicación informática o herramienta tecnológica utilizada. Por ello, en cada caso, habrá que analizar cuál es la medida que maximiza el acceso a la información, sin afectar de manera desproporcionada otros derechos e intereses.

JUEZ CONSTITUCIONAL-Deber de garantizar el respeto a los derechos fundamentales

---

REPÚBLICA DE COLOMBIA

CORTE CONSTITUCIONAL

Sala Novena de Revisión

SENTENCIA T-067 DE 2025

Ref.: Expediente No**.** T-8.202.533

Acción de tutela formulada por el ciudadano Juan Carlos Upegui Mejía contra de la Agencia Nacional Digital

-AND, el Instituto Nacional de Salud -INS-[1] y el Ministerio de Salud y Protección Social[2].

Magistrada Ponente:

Natalia Ángel Cabo

Bogotá, D.C., 26 de febrero de 2025.

La Sala Novena de Revisión de la Corte Constitucional, integrada por la magistrada Natalia Ángel Cabo, quien la preside, la magistrada Diana Fajardo Rivera y el magistrado Jorge Enrique Ibáñez Najar[3], en ejercicio de sus competencias constitucionales, legales y reglamentarias, profiere la siguiente:

SENTENCIA.

Esta decisión se emite en el proceso de revisión de los fallos de tutela dictados, en primera instancia, por el Juzgado 64 Administrativo de Oralidad del

---

[1] Vinculado al trámite de la acción de tutela mediante auto del 12 de enero de 2021, proferido por el Juzgado 64 Administrativo de Oralidad del Distrito Judicial de Bogotá, dentro del trámite de la primera instancia en el proceso de la referencia.

[2] Vinculado al trámite de la acción de tutela mediante auto del 31 de enero de 2022, proferido por la Corte Constitucional, dentro del trámite de revisión en el proceso de la referencia.

[3] Registro de proyecto: 18 de marzo de 2022. Los artículos 1 del Acuerdo 01 de 2022, 7 del Decreto 1265 de 1970 y 9 del Acuerdo 108 de 1997 establecen que se mantendrá la conformación de las Salas y su competencia durante el año, a pesar del ingreso de nuevos magistrados o magistradas que alteren el orden alfabético, pero variarán en el siguiente año calendario. El parágrafo transitorio del artículo 1º del Acuerdo 01 de 2022 regula la competencia de las Salas de Revisión de Tutelas, tras la modificación de las mismas por dicho acto administrativo y la incorporación de nuevos magistrados y magistradas a esta Corporación. De conformidad con esa disposición, las salas conformadas antes del cambio de composición mantendrán su competencia para conocer los procesos en los que se radicó el proyecto de sentencia antes del 19 de diciembre de 2022.

Distrito Judicial de Bogotá, el 18 de enero de 2021 y, en segunda instancia, por el Tribunal Administrativo de Cundinamarca, Sección Segunda, Subsección "A", el 25 de febrero de 2021, dentro de la acción de tutela promovida por el ciudadano Juan Carlos Upegui Mejía en contra de la Agencia Nacional Digital.

Síntesis de la decisión

La Sala Novena de Revisión estudió la acción de tutela instaurada por el ciudadano Juan Carlos Upegui Mejía en contra de la Agencia Nacional Digital, el Instituto Nacional de Salud y el Ministerio de Salud y Protección Social por la vulneración de su derecho fundamental al acceso a la información pública. Esto debido a que las entidades accionadas negaron su solicitud de publicar el código fuente de la aplicación CoronApp.

Las autoridades accionadas afirmaron que la información que solicitó el actor estaba amparada bajo reserva de confidencialidad, debido a que: (i) comprometía la intimidad de los datos personales que recopila la aplicación por la exposición a posibles riesgos frente a terceros malintencionados que podrían acceder a la información (artículo 18, Ley 1712 de 2014, excepción por daño a intereses de particulares); y (ii) esta era necesaria para salvaguardar la seguridad de las medidas de salud pública que se adoptaron para atender la pandemia por el Covid19 (artículo 19, Ley 1712 de 2014, excepción por daño a intereses de particulares). Adicionalmente, (iii) las autoridades accionadas alegaron que se podrían ver comprometidos sus derechos de autor, al ser quienes desarrollaron la aplicación.

Al conocer la acción de tutela, los jueces de primera y segunda instancia negaron el amparo solicitado por el actor. En esencia, adujeron que si se accediera a la petición del demandante, se pondría en riesgo información sensible de los ciudadanos que tienen registrados sus datos personales en la aplicación. Además, consideraron que se trataba de aspectos meramente técnicos y especializados, razón por la que era preciso actuar con la mayor cautela posible.

Al examinar las decisiones, tanto de las autoridades accionadas como de los jueces de tutela que conocieron del proceso, la Corte concluyó que se había vulnerado el derecho fundamental al acceso a la información pública del actor.

Por un lado, la Sala constató que las autoridades administrativas accionadas no cumplieron con la carga de identificar el fundamento legal de la reserva de la información invocada. Tampoco cumplieron con la carga argumentativa y probatoria que acredite que revelar información genera un daño presente, real, probable y específico que excede el beneficio que representa publicar la información (artículo 28, Ley 1712 de 2014).

En este punto del examen, la Sala evidenció que la justificación presentada por las entidades demandadas no era suficiente para negar la publicación del código fuente de la aplicación CoronApp. En concreto, la Corte constató que era posible tomar medidas de seguridad sobre las bases de datos en las que reposaba la información de los usuarios (p. e. separar la información, generar credenciales de acceso, contraseñas de seguridad, medios de autenticación, etc.), de tal forma que la publicación del código no comprometiera la información y los datos de las personas. Además, la Sala reiteró que, en todo caso, las entidades accionadas debían actuar con debida diligencia y cumplir con las obligaciones de custodia de la información.

Por otro lado, la Corte recordó que los jueces constitucionales son garantes del derecho fundamental al acceso a la información pública en virtud de los mandatos constitucionales y estatutarios en la materia (artículo 27, Ley 1712 de 2014). Específicamente, señaló que los jueces tienen la obligación de pronunciarse sobre los requisitos que debe cumplir una decisión que invoca la reserva sobre información pública para establecer si se acreditan las exigencias previstas por la jurisprudencia constitucional y las normas estatutarias (test de admisibilidad de la reserva).

Así, la Sala llamó la atención de los jueces de instancia porque aceptaron, sin la debida ponderación, que frente a aspectos técnicos o especializados y en

circunstancias de duda o vacío legal, proceda la negación del derecho al acceso a la información, en contravía del principio de maximización de la publicidad y de la buena fe.

Finalmente, en esta providencia la Sala adoptó algunas medidas dirigidas a que se materialice el principio de transparencia algorítmica como parte del derecho de acceso a la información pública. Estas medidas están encaminadas a que el Estado desarrolle estrategias para incrementar la disponibilidad de la información sobre los sistemas de algoritmo en los que se sustentan las herramientas tecnológicas para la actuación estatal, como aplicaciones o sistemas de decisión automatizada. Lo anterior, en aras de que la sociedad pueda tener suficientes elementos para valorar su uso y rendimiento.

I. ANTECEDENTES

1. Hechos

1. El 6 de agosto de 2020, el ciudadano Juan Carlos Upegui Mejía presentó una petición ante la Agencia Nacional Digital (AND), con el fin de obtener una información que considera de carácter público respecto a la aplicación electrónica CoronaApp.[4] Dentro de la información requerida, el actor solicitó lo siguiente:

(i) Copia del código fuente de la aplicación CoronApp en su versión actual, con el registro de cambios en el sistema de control de versiones -VCS- que utilicen (GIT, SVN o análogos);

(ii) Subsidiariamente, en caso de que no se utilice sistema de control de versiones, copia del código fuente de la aplicación en su

[4] Expediente digital T-8202533, demanda de tutela, anexo con radicado AND-EXT00345.

primera versión con el nombre de CoronApp y de todas las versiones posteriores hasta la actual (…).[5]

2. El 14 de octubre de 2020, la AND negó la solicitud de información. La entidad señaló que el acceso a la copia del código fuente de la aplicación CoronApp, así como a sus modificaciones y actualizaciones, podría comprometer la privacidad de la información personal de los usuarios de la aplicación. Por tanto, consideró que se trataba de información con carácter reservado. Adicionalmente, indicó que la aplicación CoronApp era un programa en desarrollo y constantemente recibía actualizaciones y modificaciones. Según la AND, por esta razón, la aplicación no podía ser considerada como un producto terminado y, por ende, la información solicitada no podía ser publicada.

3. El 19 de octubre de 2020, el actor presentó un recurso de reposición en contra de la decisión de la AND que negó el acceso a la información solicitada[6]. El actor sostuvo que se debían seguir los lineamientos de la Ley 1712 de 2014[7], en particular los principios de máxima publicidad y transparencia respecto al derecho al acceso a la información pública. También señaló que la AND no indicó las disposiciones constitucionales y legales que sustentan la supuesta reserva y tampoco cumplió con la carga argumentativa para justificar por qué la información solicitada es de acceso restringido. Por último, el demandante indicó que en su petición no solicitó los datos personales de los usuarios y que, incluso si así hubiera sido, la entidad podría haber brindado una información parcial excluyéndolos.

4. El 6 de noviembre de 2020, la AND confirmó la decisión de negar el acceso a información solicitada. La agencia reiteró que si accediera a la petición se pondrían en riesgo la información sensible de los usuarios de la

---

[5] Expediente digital T-8202533, demanda de tutela, folio 2.

[6] Expediente digital T-8202533, Radicado: AND-PQRSD-00074.

[7] Ley 1712 del 6 de marzo de 2014 "Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones."

aplicación. Asimismo, justificó la negativa de compartir el código fuente de la aplicación CoronApp, en la necesidad de proteger los derechos de autor sobre el software, de los cuales es titular el Instituto Nacional de Salud.

5. Por estos hechos, el 11 de diciembre de 2020, el señor Upegui Mejía presentó una acción de tutela para obtener la protección de su derecho fundamental al acceso a la información pública. En su solicitud de amparo, el actor insistió en que la negativa de la AND de entregar la información solicitada no cumplió con la carga argumentativa que se exige para justificar dicha decisión. Para explicar la forma en que la entidad accionada vulneró sus derechos, planteó en su escrito de tutela los argumentos que se describen a continuación.

6. Primero, hizo algunas precisiones sobre la aplicación CoronApp y la definición técnica del código fuente. Así, comenzó por explicar que dicha aplicación fue desarrollada por el Gobierno Nacional como un instrumento de política epidemiológica para el control de la pandemia Covid19. Con ese fin, mediante la aplicación se registraron datos sensibles de millones de colombianos. Por ello, dice el demandante, además de ser funcional y segura en términos operativos, es necesario que el registro y archivo de esos datos esté acorde con la normatividad y la garantía de la protección de datos personales.

7. Segundo, el demandante explicó que por "código fuente" se entiende "el conjunto de instrucciones que se escriben en un lenguaje de programación para que los dispositivos o computadores puedan ejecutar un programa o presentar al usuario una página web"[8].De manera que el código de fuente no incluye información personal de los usuarios y, por ende, no puede constituir información de carácter reservado.

[8] Expediente digital T-8202533, demanda de tutela, folio 3.

8. Tercero, el actor presentó varias razones por las cuales considera que tanto la aplicación CoronApp como su código fuente deben considerarse información pública. Para empezar, señaló que dicho código es público cuando se trata de una herramienta que materializa una política pública. En ese sentido, el actor sostuvo que la información solicitada se enmarca dentro de la información mínima obligatoria que deben publicar las entidades del Estado, según el literal a) del artículo 11 de la Ley 1712 de 2014. Dicha norma señala que los sujetos obligados deben publicar de manera proactiva, entre otras cosas, los "detalles pertinentes sobre todo servicio que brinde directamente al público, incluyendo normas, formularios y protocolos de atención"[9].

9. Cuarto, el accionante indicó que el código fuente puede ser entendido como análogo a un protocolo de atención de la administración pública, esto es, un conjunto de pasos para ejecutar una función. La diferencia radica en que el código fuente está escrito en lenguaje de programación, razón por la que es un protocolo digital unívoco que no está sometido a interpretación, pues es leído por las máquinas en un solo sentido. Incluso, el accionante advirtió que la propia AND reconoció el carácter de información pública del código fuente al señalar que sería revelado cuando no se realicen más modificaciones. De manera que, la entidad, en su opinión, simplemente opone la existencia de un término de reserva que es inexistente.

10. Sobre este punto, el actor alegó que negar la publicación inmediata del código fuente es inadmisible por dos motivos. Por un lado, porque la aplicación ya estaba en funcionamiento desde hacía varios meses, razón por la que no se trata de información en preparación, sino en uso (activa y desplegada). Por el otro, porque la idea de una "versión final" que opone la AND constituye un plazo indeterminado y arbitrario, y no una excepción clara, delimitada y precisa sustentada en una norma con fuerza de ley, como lo exigen los lineamientos normativos del derecho de acceso a la información pública.

---

[9] Ley 1712 de 2014, artículo 11.a

11. Quinto, el actor señaló que el acceso al código fuente cumple los objetivos que persigue el principio de transparencia de la información. Esto, debido a que ese acceso permitiría que la ciudadanía tenga mayor control y conocimiento sobre la forma en que se toman las decisiones, se administran los datos personales y las medidas de seguridad que tiene la aplicación para garantizar el respeto por la intimidad en el manejo de esos datos, de acuerdo con lo previsto en los principios generales de la Ley estatutaria de habeas data (Ley 1581 de 2012).

12. Finalmente, el demandante precisó que el derecho fundamental al acceso a la información pública ha sido reconocido por la jurisprudencia de la Corte Constitucional, en las sentencias C-491 de 2007 y C-274 de 2013, y por la legislación en la materia, particularmente por la Ley 1712 de 2014. Sobre esta última norma, el actor hizo referencia a los artículos 4 (concepto del derecho), 24 (titular del derecho), 2 (principios de máxima publicidad), 3 (principio de transparencia), 28 (carga de la prueba para las autoridades públicas cuando alegan la existencia de las reservas previstas en los artículos 18 y 19), y 21 (posibilidad de divulgación parcial de la información).

13. Por todo lo anterior, el actor solicitó al juez constitucional ordenar a la AND que le suministre la información requerida, en específico, el código fuente de la aplicación CoronApp, así como el registro de versiones o cambios que ha tenido desde su creación. Para el demandante, la entidad no podía oponer el carácter reservado de la información sin cumplir la carga argumentativa y probatoria para negar el acceso a una información pública.

2. Trámite procesal de la acción de tutela en sede de instancias y contestación de las entidades accionadas

14. Mediante el auto del 14 de diciembre de 2020[10], el Juzgado 64 Administrativo de Oralidad del Distrito Judicial de Bogotá admitió la

[10] Expediente digital T-8202533, anexo radicado "33_AUTO ADMISORIO (2)".

demanda y ordenó notificar al director de AND para que ejerciera su derecho de defensa. Adicionalmente, a través del auto del 12 de enero de 2021, dicho juzgado vinculó al trámite al Instituto Nacional de Salud (INS).

2.1. Agencia Nacional Digital –AND–

15. El 16 de diciembre de 2020[11], la AND manifestó que le informó al accionante que la aplicación CoronApp cuenta con una versión iOS y una versión Android. Respecto de la versión iOS, la entidad señaló que la desarrolló integralmente sin implementar la licencia GNU-GPL 3.0[12], en virtud del memorando de entendimiento suscrito con el Instituto Nacional de Salud (INS). Indicó, además, que los derechos de autor sobre el software están en cabeza de esta última entidad y, por ello, optó por no publicar el código fuente.

16. En relación con la versión Android, advirtió que esta es producto de una modificación al software original que se realizó bajo la licencia internacional GNU y el código fuente fue entregado por el INS a la AND. La entidad agregó que, para el momento de la contestación, del código original quedaba menos del 6%, debido a las modificaciones y ajustes que se adelantaron durante la pandemia para responder a las necesidades que se presentaron.

17. Por otro lado, la agencia resaltó que el código en cuestión se mantenía en constante actualización para cumplir con las necesidades cambiantes y proteger la información recolectada de los usuarios. Además, la AND destacó que, en consideración a la sensibilidad de los datos personales que maneja la aplicación, tomó las medidas que consideró necesarias para garantizar el

---

[11] Expediente digital T-8202533, anexo radicado "50_ Contestación tutela CoronApp"

[12] GNU (Licencia Pública General por sus siglas en inglés) es una una licencia publica general, desarrollad por primera vez en 1989, con el propósito de desarrollar un programa informático. Bajo esa licencia, cualquier persona natural o jurídica puede crear, modificar o compartir una aplicación digital abierta. El GNU es una manifestación del *copyleft,* un movimiento que aboga por la cesión de derechos de forma libre sin que se apliquen las restricciones propias de los derechos de autor y propiedad intelectual.

cumplimiento de los principios señalados en las leyes 1712 de 2014 (artículo 24, numeral 3) y 1581 de 2012[13], sobre tratamiento de datos personales.

18. En ese sentido, la entidad indicó que las modificaciones que se hacen a la aplicación implican que, a la fecha, no exista una versión completamente segura que mitigue todas las amenazas a la información personal de los usuarios. Por este motivo, la AND insistió en que la publicación del código fuente "permitiría la explotación de las vulnerabilidades que aún existen" y habilitaría a personas sin autorización para acceder a la información personal registrada por los ciudadanos o entorpecer la prestación del servicio para el que fue diseñada la aplicación.

19. Por ello, la AND afirmó que, independientemente de que se hayan respetado todos los protocolos de protección de datos personales, actualmente la versión del código fuente tiene vulnerabilidades que ponen en peligro la información personal recolectada y se incrementa el riesgo de que esa información se use de forma maliciosa. Por lo anterior, la entidad accionada consideró impertinente la solicitud de publicación del código fuente y manifestó que evaluaría la posibilidad de publicarlo únicamente cuando se encuentre terminado y no implique un riesgo para los usuarios. Adicionalmente, la agencia explicó que trabajaba en mejoras a la seguridad de la aplicación con el objetivo de materializar su deber de custodia y protección de los datos personales de los usuarios registrados.

20. En su escrito, la AND también precisó que si bien los desarrollos de la aplicación corresponden a bienes de naturaleza pública esto no equivale a decir que ostentan el carácter de bienes de uso público. En consecuencia, según lo dicho por la AND, es deber de la entidad proteger los derechos de propiedad intelectual y de autor que surgen de su desarrollo, así como la privacidad y seguridad de los datos registrados por los usuarios de la

[13] Ley Estatutaria 1581 del 17 de octubre de 2012, "Por la cual se dictan disposiciones generales para la protección de datos personales."

aplicación. La agencia destacó que era imprudente e inoportuno publicar el código fuente de la aplicación, dado que a la fecha de la contestación se tenían 13'497.917 descargas y se contaba con 3'812.995 usuarios activos. De manera que constituiría un riesgo la posibilidad de una clonación (*fishing*) de la aplicación, que permitiera modificar funcionalidades para obtener los datos personales de los ciudadanos de forma inescrupulosa.

21. En suma, la AND consideró que, en atención al tipo de información recolectada a través de CoronApp, era necesario mantener el código fuente temporalmente en reserva, pues la aplicación administra información sensible y su publicación constituye un grave riesgo. Por lo tanto, decidió que negar su publicación, al ser una decisión que está debidamente sustentada y que no vulnera el derecho de acceso a la información pública del accionante.

2.2. Instituto Nacional de Salud –INS–

22. El 13 de enero de 2021[14], el INS contestó la solicitud de amparo constitucional. Señaló que, por su función misional, adelantaba el tratamiento de datos sensibles de los ciudadanos con estricto apego a los principios y reglas establecidos en la Ley 1581 de 2012 sobre tratamiento de datos personales.

23. El INS indicó que, a través de la Resolución 1607 de 2014, adoptó el reglamento de propiedad intelectual y la política para la protección de datos personales establecida en la ley antes mencionada. Adicionalmente, señaló que en la Resolución 457 de 2020 estableció los lineamientos y objetivos de la política de protección de datos personales de la entidad.

24. En cuanto a la solicitud de entrega del código fuente de la aplicación CoronApp, el INS manifestó que, tal como lo señaló la AND, la publicación

[14] Expediente digital T-8202533, anexos radicados "48_CONTESTACION ENVIO" y "49_CONTESTACION TUTELA 2020-00203 JUAN CARLOS UPEGUI MEJÍA".

de esta información puede suponer graves riesgos. En particular, puede hacerla susceptible a ataques, razón por la que consideró prudente que dicha publicación se efectuara únicamente en el momento en el que la aplicación se encontrara terminada. En relación con las amenazas, la entidad destacó el riesgo ante potenciales hackers quienes podrían realizar ingeniería inversa de la aplicación para descifrar el algoritmo, abusar del sistema y acceder a la información personal de los ciudadanos.

25. En línea con lo anterior, el INS precisó que cuando un código es de interés nacional, como en el caso de CoronApp, se deben tomar todas las medidas suficientes para evitar la afectación de la seguridad nacional y la vulneración de la confidencialidad de la información gubernamental. Por ello, el instituto explicó que CoronApp es la única aplicación del gobierno nacional que permite a los ciudadanos acceder a la información actualizada y veraz sobre la emergencia sanitaria por la pandemia de la Covid 19, de manera que esta información se puede ver comprometida al publicar su código fuente y, si esto sucede, afectar directamente la salud y la seguridad nacional.

26. Así las cosas, el INS concluyó que, de acuerdo con lo expuesto, era prudente y oportuno mantener el código temporalmente en reserva y reiteró que, una vez se lograra la versión definitiva, el código sería publicado.

3. Sentencia de tutela de primera instancia

27. Mediante el fallo del 18 de enero de 2021[15], el Juzgado 64 Administrativo de Oralidad del Distrito Judicial de Bogotá negó el amparo solicitado. El juzgado consideró que las respuestas de las entidades demandadas cumplían las exigencias legales en relación con un posible daño a los derechos de las personas, según lo dispuesto en el artículo 18 a) de la Ley 1712 de 2014.

---

[15] Expediente digital T-8202533, anexo radicado "4_2020-00203 fallo de primera instancia".

28. Además, el juez de primera instancia señaló que, dada la sensibilidad de la información que se gestionaba a través de la aplicación CoronApp, la publicación del código de fuente podía generar un eventual daño al derecho a la intimidad de los ciudadanos. Por lo anterior, la decisión de no publicar el código fuente obedecía a un criterio de responsabilidad y cautela en la gestión pública.

29. En su sentencia, el juez administrativo indicó que la aplicación debía ser entendida como una herramienta de política pública con la que el Estado gestiona y toma decisiones de cara a la mitigación de la pandemia Covid 19. De igual modo, señaló que se trataba de un asunto relacionado directamente con decisiones en materia de salud pública, circunstancia que quedaba cobijada por lo dispuesto en el literal i) del artículo 19 de la Ley 1712 de 2014 para denegar la publicación de la información.

30. De la misma manera, el juez consideró que la AND había sido clara en advertir que, si bien implementó políticas de tratamiento de datos personales en cumplimiento de los mandatos legales vigentes, la publicación del código fuente de la aplicación podría acarrear, entre otras consecuencias, que los datos sensibles de los ciudadanos resulten expuestos a eventuales riesgos.

31. Finalmente, el juez de tutela agregó que, desde el punto de vista técnico, no era claro si la publicación del código fuente generaría eventuales riesgos para la información sensible de los ciudadanos que registran allí sus datos personales. De manera que, al tratarse de aspectos meramente técnicos y especializados, según lo expuesto por la entidad accionada, era preciso actuar con la mayor cautela posible.

32. Por lo anterior, el juzgador de primera instancia concluyó que la AND no vulneró los derechos del accionante, pues contestó de fondo sus solicitudes y decidió no publicar la información requerida, bajo el amparo de las excepciones legalmente establecidas para el efecto.

4. Impugnación

33. El accionante impugnó en tiempo el fallo de primera instancia[16], por considerar que el juez no analizó la totalidad el derecho de acceso a la información pública de forma integral. En particular, el demandante sostuvo que no se efectuó el test de daño procedente para, eventualmente, negar el acceso a la información.

34. Adicionalmente, el actor afirmó que en su petición no solicitó información personal, razón por la que no se compromete el derecho a la intimidad ni tampoco solicitó que se revelara información que pudiera afectar la salud pública. Por ello, el accionante reiteró que, según lo dispuesto en la Ley 1712 de 2014, toda restricción al derecho al acceso a la información pública es excepcional, pues debe estar contenida en una ley o en la Constitución, y debe responder al cumplimiento de finalidades legítimas y a la debida carga argumentativa.

35. En este sentido, en opinión del demandante, cualquier entidad pública, al oponer alguna excepción contenida en los artículos 18 y 19 de la precitada ley, debe indicar con claridad la norma que establece la reserva y cómo con esta se protege algún interés legítimo. En este caso en particular, las entidades demandadas debían aportar la prueba que justificara y demostrara la presencia de un daño probable, específico y significativo que excediera el interés público que subyace al acceso a la información pública.

36. El actor alegó que en ninguna de las respuestas a sus peticiones la AND probó que al revelar el código fuente de la aplicación CoronApp se generara algún riesgo inminente a la intimidad de terceros. Adicionalmente, la entidad accionada no se pronunció sobre la posibilidad de permitir el acceso a la información de forma parcial, esto es, la posibilidad de excluir aquella información que no fuera objeto de reserva.

---

[16] Expediente digital T-8202533. Escrito de Impugnación de fecha 22 de enero de 2021.

37. Por esta razón, el accionante cuestionó el fallo de primera instancia y consideró que el juez no garantizó el derecho al acceso a la información pública, debido a que se limitó a avalar las contestaciones de la AND y del INS que mencionaban superficialmente una posible afectación a la salud pública y a la seguridad nacional. En este sentido, enfatizó en que la accionada no probó los posibles riesgos de seguridad por la publicación del código fuente de la aplicación, pues únicamente se limitó a enunciarlos.

38. El señor Upegui Mejía reiteró que al entregar el código fuente de la aplicación no se ponían en riesgo los datos personales de los usuarios, debido a que el código es anterior a la entrada en operación de la aplicación y los datos de los usuarios están ubicados en bases de datos que no se solicitaron. De manera que, si existen datos personales en el código, los mismos pueden ser editados.

39. En lo que respecta a los alegados riesgos asociados a la publicación del código fuente, el accionante señaló que son infundados, pues para duplicar la aplicación con fines ilegales, como capturar información personal con fines de lucro o de suplantación personal, no se requiere el código fuente, pues la clonación consiste en simular una aplicación para que parezca real. Así, indicó que, si bien las aplicaciones pueden tener vulnerabilidades debido a la publicación del código fuente, las mismas son conocidas por la AND y el INS, quienes estaban obligadas a corregirlas.

40. Finalmente, el actor argumentó que el código fuente de aplicaciones similares a CoronApp ya había sido publicado en otros países, sin necesidad de mayores requerimientos y por mandato del principio de transparencia en la actuación administrativa. Por lo anterior, insistió en que no existe razón para que Colombia no adopte la misma determinación.

41. En consecuencia, el señor Upegui Mejía solicitó que se revocara el fallo de primera instancia y se accediera a las pretensiones del amparo.

5. Sentencia de tutela de segunda instancia

42. Mediante fallo del 25 de febrero de 2021[17], el Tribunal Administrativo de Cundinamarca, Sección Segunda, Subsección A, confirmó la decisión de primera instancia.

43. El Tribunal consideró que la decisión de las entidades accionadas se sustentó en dos argumentos. Primero, la normatividad sobre protección de datos personales y el derecho de petición, en particular el numeral 3 del artículo 24 de la Ley 1437 de 2011 que señala que está sometida a reserva toda información "que involucre derecho a la privacidad e intimidad de las personas"[18]. Segundo, la existencia de derechos de autor que se verían irrespetados con la publicación del código fuente.

44. Con base en los anteriores argumentos, el Tribunal concluyó que la publicación del código fuente de la aplicación pondría en riesgo la seguridad de la información que al menos 13 millones de ciudadanos han depositado en ella, de los cuales 3 millones eran usuarios activos. Así, destacó que entre la AND y el INS existía un acuerdo de confidencialidad y transmisión de la información que obligaba a las entidades a guardar la información que administraban, particularmente, la información de terceros. En consecuencia, era razonable la negativa de esas entidades de publicar el código fuente, pues esto podría conllevar a fallos de seguridad que permitieran el acceso a datos de los ciudadanos.

45. Para explicar este último punto, el Tribunal citó un informe que solicitó al equipo técnico de sistemas de esa corporación judicial, en el que preguntó por posibles efectos y riesgos de la publicación del código fuente y de los cambios en sus versiones. Con base en este informe, concluyó que el código

---

[17] Expediente digital T-8202533. Archivo radicado "53_ fallo dejusticia"

[18] Ley 1755 de 2015. Artículo 24, numeral 3.

fuente no contiene datos personales de los usuarios de la aplicación, pero que sí existía un riesgo de seguridad para la aplicación y los datos, pues podía conllevar a que se encontraran fallos de seguridad desconocidos o no solucionados: "y con ello tal vez a acceder a la información personal objeto de reserva y protección."[19]

46. Por otra parte, el juez de segunda instancia señaló que la información solicitada no corresponde a cualquier tipo de información, pues se trata también de "una obra inventiva y producción intelectual de las personas, que tanto naturales como jurídicas son sujetos activos de derechos de autor sobre sus obras."[20] Lo anterior, debido a que las diferentes versiones de la aplicación (Android y iOs) eran desarrollos tecnológicos de software protegidos por la normatividad de derechos de autor. Por todo lo anterior, el Tribunal concluyó que "las respuestas ofrecidas por la accionada para negar el acceso al código fuente de la CoronApp son suficientes para no vulnerar el núcleo básico del derecho de petición ni del acceso a información pública."[21]

6. Trámite en sede de revisión

47. El expediente de referencia fue escogido para revisión mediante auto del 29 de junio de 2021 por la Sala de Selección Número Seis[22], al considerar que se trata de un asunto novedoso y, por tanto, exige la necesidad de aclarar el contenido y alcance de un derecho fundamental (criterio objetivo).

48. El 5 de octubre de 2021[23], la Sala suspendió los términos del proceso para realizar una adecuada valoración del material probatorio allegado al

---

[19] Op. Cit. Expediente digital T-8202533. Archivo radicado "53_ fallo dejusticia"

[20] Ibidem.

[21] Ibidem.

[22] Conformada por la Magistrada Diana Fajardo Rivera y el Magistrado Antonio José Lizarazo Ocampo.

[23] Expediente digital, T-8202533. Archivo radicado "01AutoT-8202533PruebasOct-5-21."

proceso. Posteriormente, mediante un auto del 31 de enero de 2022[24], la Sala: (i) vinculó al Ministerio Nacional de Salud y de la Protección Social; (ii) ordenó a las entidades accionadas pronunciarse sobre aspectos de carácter técnico y científico pertinentes para resolver el objeto de debate; y (iii) requirió a la Defensoría del Pueblo y a algunas universidades para que emitieran concepto dentro del presente proceso.

49. El 23 de febrero de 2022, en cumplimiento de lo ordenado, la Dirección Jurídica del Ministerio de Salud y Protección Social presentó un escrito en el que se refirió al marco jurídico sobre la protección del código fuente de CoronApp, e indicó que es una obra sujeta a derechos de patrimoniales de autor.[25]

50. Por otra parte, y en relación con el uso que se le ha brindado a la aplicación desde octubre de 2021, la Dirección indicó que "el Ministerio [de salud] dio continuidad a las funcionalidades que soportaban la aplicación", así: "(i) caracterizar a las personas contagiadas con el virus SARS CoV2 (Covid-10) y el reporte de síntomas y (ii) descargar códigos QR para observar el resultado de las pruebas de antígenos y PCR con vigencia de 3 días".[26] Asimismo, la Dirección precisó que dichas funcionalidades estuvieron en el sistema operativo Android hasta noviembre de 2021 y en iOS (sic) hasta diciembre del mismo año, y que después de esas fechas "evolucionó a la aplicación MinsaludDigital".

51. Asimismo, la Dirección aseguró que la aplicación de CoronApp ya había cumplido su funcionalidad y que, por ello, la titularidad de los derechos patrimoniales del autor fue cedida al Ministerio de Salud y Seguridad Social. En virtud de lo anterior, ese Ministerio decidió darle un nuevo alcance y uso a la aplicación, acorde con la evolución de la pandemia y la vacunación. La

---

[24] Expediente digital, T-8202533. Archivo radicado "013AUTO T-8.202.533 Vinculación, pruebas, acceso a expediente."

[25] *Ibid*. Págs. 2 a la 10.

[26] *Ibid.* Pág. 11.

entidad indicó que para ello era necesario modificar constantemente el código fuente.

52. Así, el Ministerio indicó que esta evolución permitió unas funcionalidades distintas en la aplicación, cuya nueva versión se denomina "Minsalud Digital", entre las que se encuentra la posibilidad de descargar el certificado de vacunación. En consecuencia, el Ministerio de Salud y Seguridad Social aclaró que la aplicación no es un producto terminado, ya que se han realizado actualizaciones para que se ajuste a los cambios de la pandemia.

53. El Ministerio también explicó que Minsalud Digital es una evolución de CoronApp. En ese sentido mencionó que algunos de los cambios que diferencian a Minsalud Digital de CoronApp son los siguientes: descargar el certificado de vacunación, descargar los resultados de pruebas de antígenos y PCR, acceder a la ruta de promoción y prevención en salud, acceder a información estadística del coronavirus, realizar trámites y PQRS ante el Ministerio de Salud, y la apropiación de la imagen institucional del Ministerio.

54. Finalmente, el Ministerio aseguró que no pretendía publicar el código de fuente de los aplicativos CoronApp, hoy Minsalud Digital, debido a que estos códigos de las aplicaciones: "(…) desde el análisis de seguridad de la información/digital se encuentran caracterizados como activos críticos, según los lineamientos y políticas internas, por lo cual cualquier exposición pública podría afectar la confidencialidad e integridad del Ministerio*"*.

55. En auto del 13 de mayo de 2022[27], la magistrada ponente invitó a una serie de organizaciones y universidades para que se pronunciaran sobre los riesgos asociados a la publicación del código fuente de una aplicación pública, el momento en el que se puede considerar que dicho código está en su versión final y las medidas de seguridad que pueden implementarse para garantizar la

[27] Expediente digital, T-8202533. Archivo radicado "014AUTOT-8202533PruebasMay13-22".

protección de la seguridad informática y los datos personales de los ciudadanos registrados en dichas aplicaciones, entre otros asuntos.

56. Las pruebas recaudadas, los pronunciamientos de las partes y las intervenciones realizadas por algunos ciudadanos, organizaciones y universidades reposan en los anexos de la presente decisión, los cuales hacen parte integral de la misma.

II. CONSIDERACIONES Y FUNDAMENTOS DE LA DECISIÓN

1. Competencia

1. La Corte Constitucional es competente para revisar los fallos proferidos en virtud del trámite de acciones de tutela (arts. 86 y 241.9 C.P., 33 y 34 del Decreto 2591).

2. Planteamiento del caso, formulación del problema jurídico y estructura de la decisión

2. En el presente asunto, la Sala estudia en sede de revisión la tutela presentada por el ciudadano Juan Carlos Upegui Mejía, quien alegó que la Agencia Nacional Digital -AND- vulneró su derecho fundamental al acceso a la información pública, al negarle el acceso al código fuente de la aplicación CoronApp.

3. La entidad accionada, el Instituto Nacional de Salud y el Ministerio de Salud y Protección Social, vinculados durante trámite de la tutela, argumentaron que la información solicitada tiene el carácter de reservada, por hacer referencia a asuntos de seguridad y salud pública, y por contener datos

sensibles de los usuarios. Además, adujeron que la aplicación se encontraba en continua actualización y que hasta tanto no se terminara su desarrollo no se podría revelar la información solicitada pues, de lo contrario, se podría poner en riesgo los datos sensibles de los usuarios. Finalmente, insistieron que la información solicitada también estaba protegida por tratarse de desarrollos de software amparados bajo propiedad intelectual.

4. Los jueces de primera y segunda instancia negaron el amparo al considerar que, efectivamente, se trataba de información reservada según lo dispuesto en la Ley 1712 de 2014 y consideraron suficientes los argumentos de las autoridades accionadas.

5. La Sala debe iniciar con el estudio de procedencia de la acción de tutela. En caso de que se cumplan los requisitos de aptitud, el problema jurídico que deberá resolver es el siguiente:

> ¿vulneraron la Agencia Nacional Digital, el Instituto Nacional de Salud y el Ministerio de Salud y Protección Social el derecho fundamental al acceso a la información pública de un ciudadano al negarle el acceso al código fuente de la aplicación digital CoronApp, la cual incluye información de los ciudadanos en el marco de la contención del virus Covid 19, bajo el argumento de que dicho código es de carácter reservado y que su publicación puede poner en riesgo la integridad y reserva de los datos personales administrados en dicha plataforma?

3. Procedibilidad formal de la acción de tutela

6. Con base en lo dispuesto en el artículo 86 de la Constitución y las normas que lo desarrollan en el Decreto 2591 de 1991 (arts. 1°, 5°, 6º y 10), la

jurisprudencia de esta Corte ha sostenido que para que proceda la acción de tutela se deben acreditar los requisitos de: (i) legitimación en la causa por activa[28] y por pasiva[29], (ii) la inmediatez[30] y (iv) la subsidiariedad[31].

7. En este caso, en primer lugar, se acredita la legitimación por activa, pues la acción de tutela se presentó por el titular de los derechos fundamentales cuya protección se invoca. En particular, la acción se formuló por un ciudadano que, al igual que otros, es titular del derecho al acceso a la información pública previsto en el artículo 74 de la Constitución. Esta norma establece que: "todas las personas tienen derecho a acceder a los documentos públicos salvo los casos que establezca la ley". En un sentido similar, el artículo 4 de la Ley 1712 de 2014 dispone que: "en ejercicio del derecho fundamental de acceso a la información, toda persona puede conocer sobre la existencia y acceder a la información pública en posesión o bajo control de los sujetos obligados"[32].

8. En segundo lugar, también se acredita la legitimación por pasiva. En el asunto bajo revisión, la acción de tutela se instauró en contra de la Agencia Nacional Digital -AND- y se vinculó al Instituto Nacional de Salud -INS-, que son las autoridades que presuntamente habrían vulnerado el derecho

---

[28] Esta Corte ha admitido que la legitimación en la causa por activa se acredita, siguiendo el artículo 10° del Decreto 2591 de 1991, cuando la acción de tutela se ejerce (i) de manera directa, (ii) por medio de representantes legales (caso de los menores de edad, los incapaces absolutos, los interdictos y las personas jurídicas), (iii) a través de apoderado judicial (caso en el cual el apoderado debe ostentar la condición de abogado titulado y al escrito de acción se debe anexar el poder especial para el caso o en su defecto el poder general respectivo), y (iv) por medio de agente oficioso. Ver, sentencia T-531 de 2002.

[29]. La Corte ha señalado que la acción procede contra acciones u omisiones de autoridades que tengan la aptitud legal para responder jurídicamente por la vulneración. También procede contra particulares cuando estos presten servicios públicos, o, respecto de los cuales el accionante se encuentre en situación de indefensión.

[30] La inmediatez se refiere a la oportunidad en que debe ejercerse la acción. Aunque no hay un tiempo fijo, la jurisprudencia ha indicado que debe ser razonable.

[31] La subsidiariedad implica que la tutela solo puede ser ejercida cuando no existe otro mecanismo judicial idóneo para garantizar el derecho alegado.

[32] Ley 1712 de 2014, [p]or medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones". Artículo 4.

fundamental al acceso a la información pública del actor. Estas autoridades son sujetos obligados a garantizar el derecho fundamental al acceso a la información pública, según lo dispuesto por el artículo 5 de la Ley 1712 de 2014. En particular esta norma establece que las disposiciones de la mencionada ley son aplicables a: "[t]oda entidad pública, incluyendo las pertenecientes a todas las Ramas del Poder Público, en todos los niveles de la estructura estatal"[33].

9. Por otra parte, es preciso advertir que, en ejercicio de sus competencias, la Corte Constitucional vinculó a este proceso al Ministerio de Salud y Protección Social, autoridad pública que también es sujeto obligado en relación con la garantía de acceso a la información pública. En consecuencia, se encuentra acreditado el presupuesto de legitimación por pasiva.

10. En tercer lugar, también se cumple con el requisito de inmediatez. En el asunto que ahora se analiza, la presunta vulneración surgió cuando la AND negó el acceso a la información solicitada por el demandante. Al actor se le dio respuesta definitiva a su petición el día 6 de noviembre de 2020[34], fecha en la que se notificó el recurso de reposición en contra de la contestación inicial de la AND. Por su parte, la acción de tutela fue presentada el 11 de diciembre de 2020, esto es, alrededor de 1 mes y 5 días después de la presunta vulneración de derechos, lo cual constituye un plazo razonable.

11. Finalmente, en el presente caso se cumple con el requisito de subsidiariedad. Sobre este requisito, en materia de solicitudes de amparo del derecho al acceso a la información pública, la jurisprudencia constitucional[35] y la normatividad vigente han dispuesto algunas consideraciones especiales. Así, el artículo 27 de la Ley 1712 de 2014 establece que, cuando la solicitud de información o de documentos es negada bajo el argumento de la reserva documental o de información por las causales de "seguridad y defensa

---

[33] Ley 1712 de 2014. Artículo 5.

[34] *Cfr*. Expediente digital T-8202533.

[35] *Cfr*. Sentencia T-487 de 2017.

nacional o relaciones internacionales", se puede insistir ante la jurisdicción contencioso administrativa. El parágrafo de dicho artículo aclara que, en los casos no contemplados en ese artículo -es decir, diferentes a temas de seguridad o defensa nacional o relaciones internacionales-, procederá la acción de tutela una vez se agote el recurso de reposición.

12. Al analizar el caso concreto a la luz de las anteriores reglas, se observa que la parte accionada no formuló argumentos relacionados con la seguridad, la defensa nacional o las relaciones internacionales para justificar la reserva de la información. Esta reserva la fundamentó la AND en: (i) la protección de los datos personales de los usuarios de la aplicación, (ii) el posible de riesgo de salud pública ante un uso indebido del código, y (iii) los derechos de autor y propiedad intelectual que se derivaban de su utilización. En esa medida, y a la luz del parágrafo del artículo 27 ya citado, la acción de tutela es procedente, pues el accionante agotó el recurso de reposición.

13. En consecuencia, al encontrar acreditados los requisitos de procedencia de la acción de tutela, la Sala procede a abordar el problema jurídico arriba indicado que, en esencia, implica determinar si se vulneró el derecho fundamental de acceso a la información pública del accionante. Para hacerlo, la Corte, primero, se referirá a la jurisprudencia constitucional en materia del derecho fundamental al acceso a la información pública y la protección de datos personales. Luego, la Sala hará unas breves consideraciones sobre el principio de transparencia algorítmica como elemento esencial del derecho de acceso a la información pública. Con base en esos elementos de juicio la Sala, finalmente, procederá al análisis del caso concreto.

4. El derecho fundamental al acceso a la información pública

14. Como bien lo ha señalado esta Corte[36] uno de los rasgos fundamentales de una democracia es el de velar por que la información que es relevante para

[36] *Cfr*. Sentencias C-872 de 2003 y C-274 de 2013.

la sociedad esté disponible para la ciudadanía. Es contrario a un régimen democrático una cultura del secreto en la que no exista publicidad de los actos de las autoridades y en la que toda información del Estado sea reservada.[37] Como se expresó en la sentencia C-491 de 2007:

> " (…) la garantía más importante del adecuado funcionamiento del régimen constitucional está en la plena publicidad y transparencia de la gestión pública. Las decisiones o actuaciones de los servidores públicos que no se quieren mostrar son usualmente aquellas que no se pueden justificar. Y el uso secreto e injustificado del poder del Estado repugna al Estado de Derecho y al adecuado funcionamiento de una sociedad democrática".[38]

15. Precisamente, al reconocer que somos un Estado social de Derecho, democrático y participativo el Constituyente consagró en el artículo 74 de la Constitución Política el derecho de toda persona "a acceder a los documentos públicos, salvo los casos que establezca la ley". Se trata de un derecho autónomo e independiente cuyo alcance ha sido objeto de precisiones por parte de la jurisprudencia constitucional y por organismos internacionales. Para tener un panorama adecuado del alcance, los límites y los mandatos de aplicación que corresponden al derecho fundamental al acceso a la información pública, a continuación, se recogerán los estándares internacionales y nacionales sobre la materia, que servirán en la resolución del caso concreto.

4.1. Estándares internacionales en materia del derecho al acceso a la información pública

16. La doctrina internacional de los derechos humanos ha reconocido que el derecho fundamental al acceso a la información pública está íntimamente relacionado con varios derechos humanos como la libertad de expresión, de

---

[37] *Cfr*. Sentencias C-872 de 2003 y C-274 de 2013.

[38] *Cfr*. Sentencias C-491 de 2007 y C-274 de 2013.

pensamiento y de opinión, y que su garantía es esencial para el ejercicio de otros derechos.

17. El artículo 18 de la Declaración Universal de Derechos Humanos señala que: "todo individuo tiene derecho a la libertad de opinión y de expresión; este derecho incluye el de no ser molestado a causa de sus opiniones, el de investigar y recibir informaciones y opiniones, y el de difundirlas, sin limitaciones de fronteras, por cualquier medio de expresión". En el mismo sentido, el Pacto Internacional de Derechos Civiles y Políticos[39] (PIDCP) establece en su artículo 19 que la libertad de expresión incluye "la libertad de buscar, recibir y difundir informaciones e ideas de toda índole."[40]

18. En esta misma línea, la Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura (UNESCO), en julio del año 2002[41], promulgó la Carta de Santo Domingo por el Libre Acceso a la Información Pública[42]. En este instrumento se desarrollaron distintas consideraciones entre las cuales se destaca que: (i) el acceso a la información pública es un derecho humano universal y (ii) un principio democrático que tiene relación con el derecho a la información, a la libertad de expresión y a la libertad de prensa.

---

[39] Aprobado por la Ley 74 de 1968.

[40] Pacto Internacional de Derechos Civiles y Políticos. - "Artículo 19. 1. Nadie podrá ser molestado a causa de sus opiniones. ‖ 2. Toda persona tiene derecho a la libertad de expresión; este derecho comprende la libertad de buscar, recibir y difundir informaciones e ideas de toda índole, sin consideración de fronteras, ya sea oralmente, por escrito o en forma impresa o artística, o por cualquier otro procedimiento de su elección. ‖ 3. El ejercicio del derecho previsto en el párrafo 2 de este artículo entraña deberes y responsabilidades especiales. Por consiguiente, puede estar sujeto a ciertas restricciones, que deberán, sin embargo, estar expresamente fijadas por la ley y ser necesarias para: ‖ a) Asegurar el respeto a los derechos o a la reputación de los demás; ‖ b) La protección de la seguridad nacional, el orden público o la salud o la moral públicas."

[41] Resultado de las jornadas de "Marcos Legales que garantizan y promueven el libre acceso de los ciudadanos y de los medios de comunicación a las fuentes de información pública: Análisis de casos de América" celebradas en Santo Domingo, República Dominicana

[42] En julio de 2002, la UNESCO organizó unas jornadas alrededor de los marcos legales que garantizan y promueven el libre acceso de los ciudadanos y de los medios de comunicación a las fuentes de información pública. Al final de los debates se aprobó la mencionada carta. Para este caso, la Corte utilizará el contenido de esta declaración como criterio interpretativo auxiliar pues no cumple con los requisitos jurisprudenciales para ser considerado como parte del bloque constitucional en sentido lato o estricto ya que se trata de un documento de trabajo expedido alrededor de un evento auspiciado por una organización internacional pública.

Asimismo, expuso la necesidad de que todos los países resuelvan los vacíos legislativos existentes en la materia a través de la aprobación de leyes que garanticen el acceso a la información pública.

19. Por otra parte, el artículo 13 de la Convención Americana de Derechos Humanos -CADH reconoce el derecho de acceso a la información pública[43]. Este artículo consagra el derecho a la libertad de pensamiento, de expresión y a la información, entendido como el derecho de "buscar, recibir y difundir informaciones e ideas de toda índole, por cualquier medio."[44] De manera que es obligación de los Estados americanos adoptar las medidas para que los ciudadanos puedan acceder a la información que las autoridades públicas tienen bajo su poder (obligación de respeto y garantía), así como remover las barreras administrativas y legislativas que impiden la exigibilidad y garantía de dicho derecho (deber de adecuación de las medidas internas)[45].

20. Dentro de los parámetros del sistema regional, un instrumento referente en la materia es la Declaración de Principios sobre Libertad de Expresión[46]. En ella se consagra el derecho de toda persona a acceder a la información en poder del Estado[47]. Según la Declaración, este derecho sólo puede ser limitado por mandato previamente establecido en la ley, cuando exista un peligro real e inminente para la seguridad nacional.

---

[43] Aprobada por la Ley 16 de 1972, Convención Americana sobre Derechos Humanos, "Artículo 13. Libertad de Pensamiento y de Expresión."

[44] Artículo 13 de la Convención Americana sobre Derechos Humanos.

[45] Artículos 1.1 y 2, CADH.

[46] Adoptada por la Comisión Interamericana de Derechos Humanos durante su 108° período ordinario de sesiones, en octubre de 2000. Al igual que con la Carta de Santo Domingo, la Corte utilizará el contenido de esta declaración como criterio interpretativo auxiliar ya que se trata de un documento que no cumple con los requisitos jurisprudenciales para ser integrado al bloque de constitucionalidad en sentido estricto o lato.

[47] El Comité Jurídico Interamericano mediante la resolución CJI/RES. 147 (LXXIII-0/08) ("Principios sobre el Derecho de Acceso a la Información" estableció que "[t]oda información es accesible en principio. El acceso a la información es un derecho humano fundamental que establece que toda persona puede acceder a la información en posesión de órganos públicos, sujeto sólo a un régimen limitado de excepciones".

21. En desarrollo de los mandatos convencionales, la jurisprudencia de la Corte Interamericana de Derechos Humanos (CorteIDH), los pronunciamientos de la Comisión Interamericana de Derechos Humanos (CIDH) y los informes de la Relatoría Especial de la OEA para la Libertad de Expresión han definido aspectos fundamentales del contenido del derecho a acceder a la información y sobre las condiciones que deben cumplirse para que una limitación a tal derecho resulte legítima. Así, por ejemplo, en el caso López Álvarez vs. Honduras (2006) la CorteIDH estableció[48] tres requisitos para que una limitación al derecho de acceso a la información fuera válida: (i) que esté definida en la ley; (ii) que esté destinada a proteger los derechos o la reputación de los demás, o la seguridad nacional, el orden público, la salud o la moral pública; y (iii) que sea necesaria y proporcionada para una sociedad democrática[49].

22. Así mismo, en desarrollo de los mandatos de la Declaración de Principios sobre Libertad de Expresión, la Relatoría Especial para la Libertad de Expresión publicó en el año 2010 un manual sobre el derecho de acceso a la información en el marco jurídico interamericano[50]. Este manual resume la jurisprudencia del sistema interamericano en torno al contenido y el alcance del derecho al acceso a la información y sobre los límites que deben respetarse cuando se restringe dicho derecho. Entre otras cosas, en ese documento se advierte que toda persona es titular del derecho de acceso a la información y que de él se derivan obligaciones para las autoridades de las distintas ramas del poder y de los órganos autónomos de todos los niveles de gobierno. A su vez, se indica que el Estado está obligado a: (i) responder de manera oportuna,

---

[48] CorteIDH, Caso López Álvarez Vs. Honduras, Sentencia de 1 de febrero de 2006.

[49] CorteIDH, Caso López Álvarez Vs. Honduras, Sentencia de 1 de febrero de 2006, párr. 77; y Caso Herrera Ulloa Vs. Costa Rica, Sentencia de 2 de julio de 2004, párr. 108. Igualmente, en la Opinión Consultiva OC-5 de 1985, En ese mismo sentido, consultar el caso de *Gomes* Lund y otros vs. Brasil (2010). Caso Pueblos Indígenas Maya Kaqchikel de Sumpango Y Otros vs. Guatemala. Sentencia de 6 de octubre de 2021 (Fondo, Reparaciones y Costas). Serie C 440. CorteIDH, Caso Herzog et al. v. Brazil. Sentencia de 15 de marzo de 2018 (Fondo, Reparaciones y Costas.CorteIDH, Caso I.V. vs. Bolivia, Sentencia de 25 de mayo de 2017 (Interpretación de la Sentencia de Excepciones Preliminares, Fondo, Reparaciones y Costas).

[50] Relatoria para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos (2010). El derecho de acceso a la información en el marco jurídico interamericano. Disponible en: http://www.oas.org/es/cidh/expresion/docs/publicaciones/ACCESO%20A%20LA%20INFORMACION%20FINAL%20CON%20PORTADA.pdf

completa y accesible solicitudes de acceso a la información; (ii) contar con un recurso que satisfaga el derecho de acceso a la información; y (iii) disponer de un medio judicial idóneo y efectivo para la revisión de las negativas de entrega de información[51].

23. Como se explica en este documento, a la luz de la Convención Interamericana, las limitaciones al derecho fundamental al acceso a la información pública solo pueden tener un carácter excepcional, estar consagradas expresamente en la ley y perseguir un objetivo legítimo (como por ejemplo la protección de la seguridad nacional[52]). Es por ello que cualquier restricción debe cumplir con los estándares de necesidad y proporcionalidad, estar debidamente motivada, ajustada a una temporalidad definida y condicionada a la desaparición de la causal que justifica la limitación. Finalmente, los Estados deben actuar bajo dos principios centrales: el de máxima divulgación y el de buena fe. El primero ordena que la transparencia y el derecho de acceso a la información sean la regla general y que las reservas estén sometidas a estrictas y limitadas excepciones[53]. A su vez, el principio de buena fe estipula que los sujetos obligados por el derecho al acceso a la información pública deben actuar conforme al mismo.

24. Por otra parte, la Asamblea de la Organización de los Estados Americanos (OEA) promulgó la Ley Modelo Interamericana 2.0 sobre acceso a la información pública que fue aprobada en el mes de octubre de 2020[54].

---

[51] Contenido en el literal C, puntos 1 a 4 (a-h) del manual. Ibíd., pág. 8.

[52] Específicamente en materia de la seguridad nacional, el Principio 8 de los Principios de Lima, -que fue un documento suscrito en el 2000 por los relatores especiales para la libertad de expresión y opinión de la ONU y de la OEA y otras organizaciones-, establece que las restricciones al derecho de acceso a la información por motivos de seguridad nacional sólo serán válidas cuando estén orientadas a proteger la integridad territorial del país y en situaciones excepcionales de extrema violencia que representen un peligro real e inminente de colapso del orden democrático.

[53] Sobre este principio se puede consultar: Corte I.D.H., *Caso Claude Reyes y otros*. Sentencia de 19 de septiembre de 2006. Serie C No. 151, párr. 58c.

[54] Disponible en: https://www.oas.org/es/sla/ddi/docs/publicacion_Ley_Modelo_Interamericana_2_0_sobre_Acceso_Informacion_Publica.pdf

Este compendio de normas busca fomentar mejores prácticas en la promoción del derecho al acceso a la información. En esa vía, señala los derechos que tiene toda persona en relación con la solicitud de información ante cualquier autoridad pública[55], propende por la difusión proactiva de información a cargo de los sujetos obligados[56] y señala la clase de información clave sujeta a difusión[57]. Adicionalmente, establece una serie de excepciones en las cuales se puede negar el acceso a la información pública[58]. Sobre este último punto, el modelo propone dos categorías de excepciones a la divulgación: (i) información reservada, que comprende aquella que se excluye temporalmente del conocimiento del público por existir un riesgo claro de daño; y (ii) confidencial, que cobija datos de carácter privado en poder de sujetos obligados cuyo acceso público se prohíbe por expreso mandato constitucional o legal.

25. Por otra parte, en el derecho comparado, varios tribunales constitucionales latinoamericanos también han coincidido en la importancia del acceso a la información pública como eje del Estado de Derecho y de la democracia constitucional[59]. Así, se ha consolidado un estándar de transparencia activa según el cual las acciones del Estado y de los funcionarios públicos deben estar sometidas a un intenso escrutinio público con dos propósitos de relevancia democrática. Primero, una sociedad democrática permite y anhela que los ciudadanos puedan conocer cómo se toman las decisiones de política pública que los afectan. Segundo, este escrutinio tiene la bondad de abonar el terreno para el ejercicio adecuado de otros derechos fundamentales tales como la libertad de expresión, pensamiento y opinión. De esta manera, los jueces de la región han concluido que el acceso a la

[55] Artículo 3.

[56] Artículo 5.

[57] Artículo 6.

[58] Artículos 25 a 49.

[59]Sobre el particular, pueden consultarse, entre otras, las decisiones de Corte Suprema de la Nación Argentina. Asociación Derechos Civiles c/EN PAMI, p. 21; Tribunal Constitucional de Chile. Rol 634.2006. Sentencia del 9 de agosto de 2007, pp. 28 a 31; Corte Suprema de la Nación Argentina. Asociación Derechos Civiles c/EN PAMI, p. 21. Tribunal Constitucional de Chile. Rol 634.2006. Sentencia del 9 de agosto de 2007, pp. 28 a 31. Sala Constitucional de la Corte Suprema de Justicia. Expediente 05.001007.0007-CO Res. 2005-04005. 15 de abril de 2005

información pública permite el control de la actividad pública y fortalece el ejercicio de la democracia, siempre que ello no atente contra la seguridad del Estado y sus fines propios y legítimos.

26. Finalmente, cabe destacar lo dicho por el Tribunal Europeo de Derechos Humanos[60] en materia de restricciones a las libertades informativas, asunto relacionado con la presente controversia. Sobre ellas, dicho tribunal ha indicado que no pueden establecerse ni aplicarse restricciones de una forma que termine siendo contraproducente para el fin de proteger derechos como el acceso a la información. En esa misma línea, en relación con la información sobre programas digitales, el Comité Europeo de Protección de Datos ha dicho que: "[p]ara asegurar su equidad, la rendición de cuentas y, más en general, su consonancia con la ley, los algoritmos deben ser auditables y han de ser revisados periódicamente por expertos independientes. El código fuente de la aplicación debe hacerse público con miras a un control lo más amplio posible"[61].

4.2. Marco normativo y jurisprudencial del derecho al acceso a la información pública en Colombia

27. El acceso a la información pública constituye un aspecto cardinal dentro de una democracia constitucional, pues se trata de un derecho fundamental autónomo[62] que tiene como finalidad lograr la mayor publicidad y

---

[60] *Cfr*. Tribunal Europeo de Derechos Humanos, *Bayev and Others v. Russia*, 20 de junio de 2017, Rad. 67667/09, 44092/12 y 56717/12 (párr. 83).

[61] *Cfr*. Comité Europeo de Protección de Datos, Directriz 04/2020 sobre el uso de datos de localización y herramientas de rastreo de contactos en el contexto de la pandemia de COVID-19, adoptada el 21 de abril de 2020.

[62] *Cfr*. Sentencias T-473 de 1992, T-695 de 1996, T-074 de 1997, C-491 de 2007 y C-274 de 2013. Como se citó en la sentencia C-274 de 2013, la sentencia T-705 de 2007 precisó que el precedente constitucional en esta materia: "ha establecido que de la interpretación sistemática del derecho de petición (Art. 23 C.P.) y el libre acceso a los documentos públicos (Art. 74 C.P.), así como de las normas que integran el bloque de constitucionalidad, en especial, los artículos 13 de la Convención Interamericana sobre Derechos Humanos y 19 del Pacto Internacional de Derechos Civiles y Políticos se deriva el derecho fundamental de acceso a los documentos públicos."

transparencia de las actuaciones del Estado. Es, además, un medio para que los ciudadanos conozcan las actuaciones de las autoridades y puedan ejercer control sobre su actuación. De manera que el derecho de acceso a la información pública no se limita simplemente a los trámites cotidianos que desarrollan los ciudadanos frente a la administración pública, sino que se relaciona con actuaciones en las que se compromete algún elemento esencial de la democracia y el ejercicio de derechos fundamentales. Incluso se convierte en una herramienta trascendental en casos en los que es necesario conocer la verdad frente a graves violaciones de derechos humanos.

28. En atención a su trascendencia, como ya se indicó, el artículo 74 de la Constitución, reconoce el derecho al acceso a la información pública, al disponer, en su inciso primero, que "todas las personas tienen derecho a acceder a los documentos públicos salvo los casos que establezca la ley." También como se mencionó, pero vale la pena reiterarlo, este derecho, si bien es de carácter autónomo, está ligado a otras garantías fundamentales, como la libertad de expresión, el derecho a informarse y recibir información veraz e imparcial[63], el derecho de petición y el de habeas data, entre otros. Sobre este trascendental derecho, la Corte se ha pronunciado en diferentes oportunidades y ha fijado reglas sobre su alcance. A continuación, se describe ese desarrollo jurisprudencial.

4.2.1. Parámetros jurisprudenciales en materia del derecho fundamental al acceso a la información pública

29. En el inicio de su jurisprudencia, esta Corte se pronunció sobre la naturaleza y alcance del derecho fundamental al acceso a la información pública. Así, por ejemplo, en la sentencia T-473 de 1992 precisó que si bien este derecho podría entenderse como parte del núcleo esencial del derecho de petición, era esencial reconocer su carácter autónomo, por expresa disposición de la Constitución. Esta apreciación fue recogida por la Corte en otras de sus

[63] Como indicó este Tribunal Constitucional en la sentencia C-274 de 2013, el derecho a acceder a información pública es instrumento necesario para el ejercicio del derecho a la libertad de expresión y, además, ambos derechos comparten su núcleo axiológico.

primeras decisiones, en las que se enfatizó que si bien el acceso a la información pública comparte su núcleo axiológico con otros derechos (como el de petición, a la información y a la libre expresión), "tiene también un contenido y alcance particulares que le otorgan especificidad y autonomía dentro del conjunto de los derechos fundamentales"[64].

30. Tras esas decisiones, el legislador expidió la Ley Estatutaria 1712 de 2014 "[p]or medio de la cual se crea la ley de transparencia y del derecho de acceso a la información pública nacional y se dictan otras disposiciones" (en adelante, ley estatutaria de información pública). Dicha ley, expresa como objetivo el de "regular el derecho de acceso a la información pública, los procedimientos para el ejercicio y garantía del derecho y las excepciones a la publicidad de información"[65].

31. En la sentencia C-274 de 2013 la Corte realizó el control previo, automático e integral de constitucionalidad de la mencionada ley estatutaria. En esa providencia, la Corte recogió las reglas jurisprudenciales establecidas hasta el momento en relación con el derecho fundamental al acceso a la información pública y se pronunció sobre los nuevos aspectos que el legislador estatutario incluyó en la regulación. Principalmente, la Corte se pronunció sobre: (i) las funciones esenciales del derecho de acceso a la información pública y los deberes de las autoridades públicas para su garantía; (ii) las subreglas jurisprudenciales sobre el alcance y las limitaciones a dicho derecho; y (iii) la interpretación conforme a la Constitución de algunos de los artículos del derecho fundamental al acceso a la información pública. Por ejemplo, en dicha sentencia, la Corte señaló que las normas que desarrollan contenidos del derecho al acceso a la información pública deben advertir que su reconocimiento cumple con unas funciones principales. Primero, una función democratizadora toda vez que garantiza la participación democrática y el ejercicio de los derechos políticos. Segundo, una función instrumental, pues su materialización habilita el ejercicio de otros derechos constitucionales, al

---

[64] *Cfr*. Sentencias T-524 de 1993 y T-621 de 1996.

[65] Ar. 1 de la Ley 1712 de 2014.

permitir conocer las condiciones necesarias para su realización[66]. Tercero, una función de transparencia de la gestión pública, ya que constituye uno de los principales instrumentos de control y veeduría ciudadana frente a la autoridad estatal.

32. Adicionalmente, y en línea con las mencionadas funciones, la Corte también ha indicado que respecto del derecho fundamental al acceso a la información pública las autoridades tienen por lo menos dos deberes correlativos. De un lado, garantizar el acceso, es decir, suministrar a quien lo solicite información clara, completa, oportuna, cierta y actualizada sobre su actividad. De otro lado, conservar un registro cuidadoso de la información sobre sus actividades misionales pues, de no hacerlo, vulnerarían el derecho en cuestión al impedir que se ejerza un control sobre sus actuaciones[67].

33. Adicionalmente, la citada sentencia reiteró las subreglas decantadas por la jurisprudencia constitucional[68] y que definen tanto el alcance como las limitaciones constitucionalmente admisibles al derecho fundamental al acceso a la información pública[69]. Estas reglas recogen los elementos constitucionales

---

[66] Por ejemplo, en la sentencia C-491 de 2007, la Corte enfatizó en cómo el derecho a acceder a documentos públicos es "una herramienta esencial para la satisfacción del derecho a la verdad de las víctimas de actuaciones arbitrarias y de violaciones de derechos humanos y para garantizar el derecho a la memoria histórica de la sociedad."

[67] Sentencia C-872 de 2003. Al respecto dijo la Corte: "en una sociedad democrática, la regla general consiste en permitir el acceso ciudadano a todos los documentos públicos. De allí que constituya un deber constitucional de las autoridades públicas entregarle, a quien lo solicite, informaciones claras, completas, oportunas, ciertas y actualizadas sobre cualquier actividad del Estado. Aunado a lo anterior, debe existir, en toda entidad oficial, una política pública de conservación y mantenimiento de esta variedad de documentos, muy especialmente, aquellos que guarden una relación directa con la comisión de violaciones masivas y sistemáticas de los derechos humanos y del derecho internacional humanitario."

[68] Estas subreglas han sido expuestas, entre otras, en las sentencias C-891 de 2002, C-872 de 2003, C-491 de 2007 y reiteradas en la sentencia C-274 de 2013.

[69] Siguiendo los lineamientos expuestos en la sentencia C-274 de 2013, la Corte ha señalado estos límites y alcances en los siguientes pronunciamientos: Esa línea jurisprudencial se encuentra en las sentencias T-473 de 1992, T-578 de 1993, T-605 de 1996, C-711 de 1996, T-074 de 1997, C-957 de 1999, T-1268 de 2001, T-729 de 2002, C-872 de 2003, C-370 de 2006, C-491 de 2007, T-157 de 2010, T-580 de 2010, C-640 de 2010, T-759 de 2010, T-161 de 2011, T-451 de 2011, T-487 de 2011, C-881 de 2011, C-540 de 2012 y C-274 de 2013.

de la publicidad y transparencia de la función pública, resaltan el papel del mencionado derecho como instrumento esencial para salvaguardar a las personas frente a posibles arbitrariedades de las autoridades públicas y reiteran que sus límites deben estar sometidos a rigurosas exigencias constitucionales. En el siguiente cuadro se resumen las subreglas jurisprudenciales desarrolladas en relación con el derecho fundamental de acceso a la información pública.

Cuadro 1: reglas jurisprudenciales para la protección del derecho fundamental de acceso a la información pública

Regla	Contenido
Regla general de acceso sin reserva.	Las personas tienen un derecho fundamental al acceso a la información que esté en poder de las autoridades. Si no existe reserva legal expresa, entonces se aplica sin restricción el derecho fundamental al acceso a la información[70].
Límites sujetos a reserva constitucional y de ley.	Por disposición del artículo 74 superior, la limitación o reserva al acceso a información de interés debe estar debidamente sustentada en la ley o la Constitución.
Claridad y precisión de la reserva.	La ley que limite el derecho fundamental de acceso a la libertad de información debe ser precisa y clara en relación con: (i) el tipo de información que es objeto de reserva, (ii) las condiciones en las que dicha reserva puede oponerse a los ciudadanos, (iii) las autoridades que pueden aplicarla y (iv) los sistemas de control que operan sobre las actuaciones que permanecen reservadas. En

[70] En la sentencia C-872-2003 la Corte Constitucional señaló que, en una sociedad democrática, la regla general es que los ciudadanos pueden acceder a los documentos públicos, a excepción de los casos en donde exista reserva legal. En esta línea indicó que constituye "un deber constitucional de las autoridades públicas entregarle, a quien lo solicite, informaciones claras, completas, oportunas, ciertas y actualizadas sobre cualquier actividad del Estado".

	consecuencia, no son constitucionalmente admisibles las restricciones impuestas por normas genéricas, vagas o ambiguas.
Reserva sobre documentos públicos	Cuando se solicitan documentos cuyo contenido está sujeto a reserva, el límite al derecho de acceso a la información pública no puede llevar a que se niegue la existencia del documento. Es decir, la reserva opera sobre el contenido mas no sobre la información de la existencia de dicho documento. Esto por cuanto los ciudadanos deben tener una oportunidad, así sea mínima, de ejercer control al poder público.
Reserva limitada a información que compromete derechos fundamentales o bienes constitucionales valiosos, pero no sobre el proceso público dentro del cual dicha información se inserta.	La reserva tiene justificación cuando envuelve datos que pueden afectar los derechos de las personas o sujetos cuya información es un bien constitucionalmente relevante[71]. En los escenarios en que es posible escindir la información sobre la cual no recae reserva de aquella protegida, es deber de las autoridades la divulgación parcial de la información[72].
Deber de motivación de la decisión de invocar la reserva.	Cualquier decisión destinada a mantener en reserva determinada información debe ser motivada.[73] La autoridad o servidor público debe motivar por escrito su decisión y señalar, de forma clara y precisa, la norma legal o constitucional que así lo autoriza y cómo su decisión se deriva de ella.
Aplicación e interpretación	La interpretación de la norma sobre reserva debe ser restrictiva y en caso de duda sobre la

[71] Así, por ejemplo, en casos de violencia contra menores de edad, son reservados el nombre o los datos que permitan su identificación, pero no el resto de la información que reposa en el proceso. Cfr. Sentencia C-274 de 2013.

[72] Cfr. Ley 1712 de 2014. Artículo 21.

[73] Cfr. Sentencia C-274 de 2013.

restrictiva de la reserva.	configuración de la reserva esta debe resolverse en favor del derecho fundamental al acceso a la información pública.
La reserva legal no cobija información que por decisión constitucional debe ser pública.	Las reservas legales no cobijan procesos y actuaciones cuya publicidad es constitucionalmente obligatoria. Dicha información debe ser pública en cualquier circunstancia, de forma tal que pueda ser conocida y controvertida por la ciudadanía.
La reserva debe ser temporal	La ley debe establecer un límite temporal a la reserva. Su plazo debe ser razonable y proporcional a la relevancia de la protección del bien jurídico constitucional que se busca proteger y vencido dicho término debe levantarse.
Sistemas adecuados de custodia de la información en reserva.	Durante el período amparado por la reserva la información debe ser adecuadamente custodiada de tal forma que resulte posible su posterior publicidad.[74] La pérdida o deterioro de los documentos en los que reposa esta información puede dar lugar a graves sanciones disciplinarias e, incluso, penales.
La reserva obliga a los servidores públicos, pero no a los periodistas.	La reserva obliga a los servidores públicos relacionados con el manejo de la información, pero no habilita al Estado para censurar la publicación de dicha información cuando los periodistas han tenido acceso a ella y pueden publicarla[75].
La reserva no puede impedir el control intra o inter orgánico, jurídico y político de las actuaciones	La reserva puede ser oponible a los ciudadanos, pero no puede convertirse en una barrera para impedir el control por parte de otras autoridades públicas. La información que se alega reservada no puede escapar al control jurídico (administrativo y

[74] Cfr. Sentencia C-370 de 2006.

[75] En aplicación de esta regla la Corte declaró inexequible una norma que prohibía a los periodistas difundir información reservada.

públicas respecto de la información.	judicial) ni político de los ciudadanos.
Razonabilidad y proporcionalidad de los límites al derecho al acceso a la información pública.	El legislador puede establecer límites al derecho fundamental al acceso a la información pública para salvaguardar derechos fundamentales o bienes constitucionalmente valiosos como la seguridad nacional, el orden público o la salud pública. Estas limitaciones deben cumplir con los estándares constitucionales de razonabilidad y proporcionalidad.
Procede el control administrativo y judicial a la decisión que alega la reserva.	Los jueces competentes deben definir si la decisión de acceder -o no- a la información por parte de un sujeto obligado se encuentra soportada de manera clara y precisa en una ley, y si cumple con los principios de razonabilidad y proporcionalidad. Los ciudadanos pueden acudir a los recursos o acciones judiciales existentes para impugnar la decisión de mantener en reserva una determinada información.
La reserva en asuntos relacionados con defensa y seguridad nacional debe cumplir con los estándares generales de las limitaciones admisibles del derecho.	Aunque la restricción del principio de publicidad de la información del Estado por la defensa de la seguridad nacional constituye una restricción legítima, la limitación que se establezca al derecho fundamental al acceso a la información pública debe satisfacer de manera rigurosa los principios de razonabilidad y proporcionalidad, así como los restantes requisitos antes mencionados.

34. Con base en lo expuesto se puede concluir que el acceso a la información pública es la regla general y que solo en algunos casos y frente a cierto tipo de información es legítima su restricción. Sin embargo, esos límites al derecho al acceso a la información pública deben sustentarse en un motivo

preciso, previamente definido en la Constitución o en la ley, y debe ser una restricción razonable y proporcional. Lo anterior, en consideración a las importantes finalidades que persigue el acceso a la información pública.

4.2.2. Parámetros normativos establecidos por la ley del derecho fundamental al acceso a la información pública.

35. Ahora bien, además de la jurisprudencia constitucional sobre el derecho fundamental de acceso a la información pública, es importante tener en cuenta algunos de los elementos de la ley estatutaria del derecho al acceso a la información pública (Ley 1712 de 2014). Estos elementos permiten establecer con mayor claridad los escenarios en los que opera el derecho, los sujetos obligados, la clasificación de la información y las reglas estatutarias que rigen sus excepciones. Como se verá en la descripción, varios de los elementos de la regulación coinciden con los parámetros o reglas jurisprudenciales, pero la referencia a estas disposiciones y conceptos permiten comprender con mayor claridad la forma en la que opera el derecho, la identificación de los sujetos obligados a garantizar el acceso y las categorías propias relevantes.

36. En primer lugar, algunas definiciones relevantes aplicables al caso concreto son las siguientes:

(i) Sujetos obligados. La ley estatutaria los define como aquellos que tienen el deber de garantizar el ejercicio pleno del derecho fundamental al acceso a la información pública, esto es, quienes deben brindar el acceso a la información solicitada. Son sujetos obligados todas las entidades y autoridades públicas, así como los particulares (personas naturales y jurídicas) que presten funciones o servicios públicos, así como los partidos y movimientos políticos, y quienes administren o manejen recursos de origen público o parafiscales[76].

[76] Ley 1712 de 2014. Artículo 5.

(ii) Información pública. Se trata de toda información que un sujeto obligado genere, obtenga, adquiera o controle en su calidad de tal[77].

(iii) Información pública clasificada. Es la información que está en poder o custodia de un sujeto obligado en su calidad de tal, pero pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica. Por lo tanto, el acceso a esta información puede ser negado o exceptuado[78].

(iv) Información pública reservada. Corresponde a aquella información que está en poder o custodia de un sujeto obligado en su calidad de tal, pero cuyo acceso se puede exceptuar por daños a intereses públicos[79].

(v) Datos abiertos. Son los datos primarios o sin procesar que se encuentran en formatos estándar o interoperables que facilitan su acceso y reutilización, los cuales están bajo la custodia de las entidades públicas o privadas que cumplen con funciones públicas.[80].

37. Ahora bien, los literales c y d del artículo 6 de la Ley 1712 de 2014, al referirse a la información pública clasificada y reservada, remiten a los artículos 18 y 19 de la misma ley, que regulan las excepciones al acceso a la información pública. Estas disposiciones establecen los criterios para determinar si una información tiene el carácter de clasificada o reservada, y, en conjunto con el artículo 28 de la ley, fijan las reglas bajo las cuales deben operar las excepciones al acceso a la información pública.

---

[77] Ley 1712 de 2014. Artículo 6.

[78] Ibidem.

[79] Ibidem.

[80] Ibidem.

38. Puntualmente, el artículo 18 se refiere a información clasificada. Textualmente, indica este artículo:

> **ARTÍCULO 18. Información exceptuada por daño de derechos a personas naturales o jurídicas.** Es toda aquella información pública clasificada, cuyo acceso podrá ser rechazado o denegado de manera motivada y por escrito, siempre que el acceso pudiere causar un daño a los siguientes derechos:
>
> a) El derecho de toda persona a la intimidad, bajo las limitaciones propias que impone la condición de servidor público, en concordancia con lo estipulado por el artículo 24 de la Ley 1437 de 2011.
>
> b) El derecho de toda persona a la vida, la salud o la seguridad;
>
> c) Los secretos comerciales, industriales y profesionales
>
> **PARÁGRAFO.** Estas excepciones tienen una duración ilimitada y no deberán aplicarse cuando la persona natural o jurídica ha consentido en la revelación de sus datos personales o privados o bien cuando es claro que la información fue entregada como parte de aquella información que debe estar bajo el régimen de publicidad aplicable

39. Es decir, la información clasificada es aquella que está en cabeza de un sujeto obligado a garantizar el acceso a la información pública, pero cuya publicación puede causar un daño a ciertos intereses porque es información que pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica. En virtud de esa potencial afectación, el acceso a esta información clasificada puede ser rechazada o denegada.

40. Esta excepción a la publicidad de la información es excepcional y debe ser interpretada de forma estricta. Por ello, al negar el acceso a esa información, el sujeto obligado debe, por escrito, "acreditar que esa reserva obedece a un fin constitucionalmente legítimo, importante y hasta imperioso, y que la restricción es razonable y proporcionada"[81]. Este deber de motivación

---

[81] Sentencia C-274 de 2013.

debe leerse, además, a la luz de lo dispuesto en el artículo 28 de la ley en mención, en donde se establece que, si se alega una de las excepciones del artículo 18, el sujeto obligado tiene la carga de demostrar que "la revelación de la información causaría un daño presente, probable y específico que excede el interés público que representa el acceso a la información."[82] Si bien más adelante la Sala ahondará en ese estándar, conocido como el test del daño, lo relevante en este punto es reiterar que la carga probatoria y argumentativa que se exige a quien niega el acceso a información por su posible afectación a intereses particulares es alta.

41. Sobre la información clasificada como límite al derecho al acceso a la información pública la Corte señaló[83] que es admisible por la necesidad de protección de otros derechos fundamentales que puedan verse afectados por la publicidad de la información. No obstante, la Corte también precisó que "la reserva legal sólo puede operar sobre la información que compromete derechos fundamentales o bienes constitucionales, pero no sobre todo el proceso público dentro del cual dicha información se inserta"[84].

42. Por su parte, el artículo 19 de la Ley 1712 de 2014 se refiere a la información reservada. Textualmente, indica lo siguiente:

> **ARTÍCULO 19. Información exceptuada por daño a los intereses públicos.** Es toda aquella información pública reservada, cuyo acceso podrá ser rechazado o denegado de manera motivada y por escrito en las siguientes circunstancias, siempre que dicho acceso estuviere expresamente prohibido por una norma legal o constitucional:
>
> a) La defensa y seguridad nacional;
> b) La seguridad pública;
> c) Las relaciones internacionales;

---

[82] Ley 1712 de 2014, artículo 28

[83] *Cfr*. Sentencia C-274 de 2013.

[84] *Cfr*. Sentencias C-274 de 2013 y C-491 de 2007.

d) La prevención, investigación y persecución de los delitos y las faltas disciplinarias, mientras que no se haga efectiva la medida de aseguramiento o se formule pliego de cargos, según el caso;
e) El debido proceso y la igualdad de las partes en los procesos judiciales;
f) La administración efectiva de la justicia;
g) Los derechos de la infancia y la adolescencia;
h) La estabilidad macroeconómica y financiera del país;
i) La salud pública.

PARÁGRAFO . Se exceptúan también los documentos que contengan las opiniones o puntos de vista que formen parte del proceso deliberativo de los servidores públicos.

43. Así, la información pública reservada es aquella cuya publicación puede generar un daño a un interés público o general. Tal y como sucede con la información clasificada, la negación o rechazo de información reservada debe hacerse de manera motivada, por escrito y tener fundamento en una norma legal o constitucional que prohíbe el acceso a esa información. Como la Corte lo precisó en la sentencia C-273 de 2013, quien niega el acceso a la información con el argumento de que es reservada, debe cumplir con la carga específica prevista en el artículo 28 de la Ley 1712 de 2014. Así, el sujeto obligado que niegue el acceso a información pública alegando su carácter reservado deberá hacerlo por escrito y demostrar, como se precisará más adelante, que existe un riesgo presente, probable y específico de generar un daño significativo[85].

44. En síntesis, las excepciones al acceso a la información pública previstas en los artículos 18 y 19: (i) son de carácter excepcional y por exigencia constitucional su interpretación es limitada; (ii) deben ser interpretadas a la luz de las demás exigencias constitucionales que aseguran que la decisión de mantener en secreto una información pública no es arbitraria ni tiene la intención de impedir el control ciudadano sobre el ejercicio del poder y de la gestión pública; (iii) en los casos en los que parte de la información contenida en un documento no esté protegida por las excepciones se deberá hacer una versión pública que mantenga la reserva únicamente sobre la información

[85] Sentencia C-273 de 2013.

exceptuada; (iv) el sujeto obligado que niegue el acceso a la información pública debe aportar las razones y pruebas que fundamentan y demuestran que la información solicitada debe permanecer en reserva[86].

El test de daño

45. Ahora bien, respecto de las obligaciones de motivación que debe cumplir quien niega el acceso a la información, la ley estatutaria contiene un artículo específico al que ya se ha hecho referencia. El artículo 28 desarrolla lo que se conoce como el test del daño, que busca equilibrar el derecho de acceso a la información pública y la protección de ciertos intereses que se pueden ver afectados por la publicación de determinada información. Para ello, la norma establece que el sujeto obligado que niegue el acceso a determinada información pública alegando un daño a un interés particular o público debe demostrar que:

a) la información está relacionada con un objetivo constitucional y legalmente legítimo;
b) se trata de una de las excepciones expresamente establecidas en los artículos 18 y 19 de la Ley 1712 de 2014;
c) la información causaría un daño presente, probable y específico sobre un bien o interés constitucional;
d) di cho daño excede el interés público que representa el acceso a la información.

46. El Decreto 103 de 2015, que reglamentó la Ley 1712 de 2014, define en el artículo 34 las características del daño. Así, dicha disposición indica que el daño es presente cuando no es remoto ni eventual; probable, cuando se demuestra que existen las circunstancias que harían posible su materialización; y específico cuando puede individualizarse de tal forma que no se trate de una afectación genérica.

---

[86] Sentencia T-330 de 2021.

47. Para que el sujeto obligado se niegue a suministrar una determinada información pública debe demostrar que el daño que podría producirse si se accediera a la petición es sustancial, es decir, que excede el interés público de darla a conocer. Para la Corte, "[l]a determinación de qué tan sustancial es un daño se determina al sopesar si el daño causado al interés protegido es desproporcionado ante el beneficio que se obtendría por garantizar el derecho a acceder a documentos públicos"[87]. En consecuencia, en la respuesta que niega el acceso a la información con base en las excepciones ya referidas, el sujeto obligado debe realizar una ponderación entre los costos y beneficios de publicar la información y explicar por qué considera que, a la luz de esa ponderación, el daño es desproporcionado.

48. En suma, los anteriores parámetros jurisprudenciales y normativos constituyen el marco de referencia del derecho de acceso a la información pública y, por lo tanto, guiarán el análisis en el caso concreto. Sin embargo, resulta igualmente necesario hacer una breve referencia a los principales lineamientos en relación con la protección de datos personales en nuestro ordenamiento jurídico, teniendo en cuenta que en el presente asunto la Agencia Nacional Digital negó el acceso al código fuente de la aplicación CoronApp, entre otras razones porque esta aplicación recolectaba datos personales.

5. La protección de datos personales en el ordenamiento jurídico colombiano. Habeas data e intimidad de la información personal

49. La jurisprudencia de esta Corte ha estudiado en diferentes oportunidades el derecho fundamental al habeas data y, en general, la protección de datos personales ante la cotidiana y masiva recolección, almacenamiento y tratamiento de la información personal en bases de datos[88]. Además de reconocer su carácter autónomo, la jurisprudencia ha destacado que el derecho a conocer la información obrante en bases de datos,

---

[87] Sentencia C-274 de 2013

[88] Al respecto se pueden consultar las sentencias T-414 de 1992, T-307 de 1999, T-729 de 2002, C-692 de 2003, C-1011 de 2008, T-161 de 2011 y, especialmente, C-748 de 2011.

actualizarla y rectificarla tiene una relación intrínseca con la protección de la intimidad, el buen nombre, el libre desarrollo de la personalidad y otros derechos, si se tiene en cuenta que el tratamiento de datos hoy permea casi todas las actividades de la vida cotidiana de los individuos.

50. Sobre el concepto de **datos personales**[89], basándose en la normatividad estatutaria, la Corte ha enfatizado en algunas características. Por ejemplo, ha indicado que los datos personales: (i) se refieren a aspectos exclusivos y propios de una persona natural; (ii) se trata de información que permite identificar a la persona, con cierto grado de certeza; (iii) su titularidad y, por lo tanto, su propiedad reside exclusivamente en la persona sobre la cual se genera el dato, así su recolección por terceros se efectúe de manera lícita; (iv) su tratamiento está sometido a reglas especiales en materia de captación, administración y divulgación[90].

51. Por su parte, en cuanto a los **datos sensibles,** la jurisprudencia ha precisado que corresponden a una categoría particular de datos que representa riesgos especiales para la persona titular y que son de interés exclusivo y excluyente del titular. Estos son datos que impactan elementos personalísimos, razón por la cual su uso indebido puede afectar la privacidad, la integridad, el libre desarrollo de la personalidad y la dignidad humana, entre otros derechos. Así mismo, estos datos pueden exponer al titular al riesgo de ser objeto de actos o políticas de discriminación o marginalización, bien sea de manera directa o indirecta[91]. Según el artículo 5 de la Ley 1581 de 2012, estos datos hacen referencia, por ejemplo, a aquellos que revelan "el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueven intereses de cualquier partido político o que garanticen los derechos y

---

[89] Los datos personales, a su vez, suelen ser clasificados en otras categorías despendiendo de su mayor o menor grado de aceptabilidad de divulgación: datos públicos, semiprivados y privados o sensibles. Sin embargo, por ser relevante para el caso solo se hará referencia a los datos sensibles.

[90] Cfr. Sentencias T-414 de 1992 y C-748 de 2011.

[91] Sentencias C-406 de 2022, T-450 de 2022, SU-139 de 2021, T-114 de 2018 y T-1003 de 1999, y artículo 5 de la Ley 1581 de 2012.

garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual y los datos biométricos".

52. Finalmente, el **tratamiento de datos** hace referencia a cualquier operación que se pretenda hacer con los datos personales, con independencia de si dicha actuación se adelanta con o sin ayuda de la informática. En materia de tratamiento, opera una prohibición general sobre la categoría de datos sensibles, cuyo tratamiento está prohibido salvo los eventos señalados en el artículo 6 de la Ley 1581 de 2012[92].

53. Ahora bien, identificadas estas categorías clave en materia de habeas data, basta señalar, para el caso concreto, que el tratamiento a los datos personales opera sobre unos principios específicos en materia de divulgación. Así, de un lado, está el principio de libertad, según el cual los datos personales no pueden ser divulgados sin previa autorización del titular o, en ausencia de su autorización, sin la existencia de un mandato legal o judicial que releve su consentimiento[93]. Este principio se complementa con el de circulación restringida, según el cual los datos personales, a excepción de 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 ley"[94]. Finalmente, está el principio de

---

[92] Ley 1581 de 2012. Artículo 6. Tratamiento de datos sensibles. Se prohíbe el Tratamiento de dados sensibles, excepto cuando: a) El Titular haya dado su autorización explícita a dicho Tratamiento, salvo en los casos que por ley no sea requerido el otorgamiento de dicha autorización; b) El Tratamiento sea necesario para salvaguardar el interés vital del Titular y este se encuentre física o jurídicamente incapacitado. En estos eventos, los representantes legales deberán otorgar su autorización; c) El Tratamiento sea efectuado en el curso de las actividades legítimas y con las debidas garantías por parte de una fundación, ONG, asociación o cualquier otro organismo sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, siempre que se refieran exclusivamente a sus miembros o a las personas que mantengan contactos regulares por razón de su finalidad. En estos eventos, los datos no se podrán suministrar a terceros sin la autorización del Titular; d) El Tratamiento se refiera a datos que sean necesarios para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial; e) El Tratamiento tenga una finalidad histórica, estadística o científica. En este evento deberán adoptarse las medidas conducentes a la supresión de identidad de los Titulares".

[93] Ley 1581 de 2012, artículo 4 literal c.

[94] Ley 1581 de 2012, artículo 4 literal f.

confidencialidad, el cual le impone a las personas que intervienen en el tratamiento de datos personales garantizar la reserva de la información[95].

54. Así, a partir de una mirada integral de los derechos de acceso a la información pública y del derecho al habeas data se advierte que sus protecciones propias están, a la vez, comprendidas en la regulación del derecho fundamental al acceso de información pública. En efecto, como se explicó ampliamente en el capítulo anterior, el legislador estatuario previó, como excepciones al acceso a la información pública, la clasificada, que está en poder de un sujeto obligado en su calidad de tal, pero cuya revelación puede generar una afectación a un interés o derecho constitucional particular como la intimidad o la vida[96].

55. A la luz de las anteriores precisiones, pasa la Corte a hacer un análisis relacionado con la información correspondiente a la programación de herramientas que permiten, entre otras cosas, la recolección masiva de datos personales, como las aplicaciones desarrolladas e implementadas por el Estado en ejercicio de sus funciones. Así, por ser relevante para el caso concreto, la Sala abordará el acceso a la información pública relacionada con la programación de aplicaciones y las reglas sobre la publicidad de los algoritmos.

6. El derecho de acceso a la información pública en el marco de sistemas de tomas de decisiones automatizadas: la transparencia algorítmica y la publicidad del código fuente.

---

[95] Ley 1581 de 2012, artículo 4 literal h.

[96] La sentencia C-274 de 2013 reconoce que las categorías del derecho fundamental al acceso a la información pública son diferentes a las de habeas data, pero que son armónicas. En ese sentido indicó que: Dado el margen de configuración con que cuenta el legislador en esta materia, es compatible con la Carta la opción tomada por el legislador. Si bien pudo haber escogido otra categorización con el fin de determinar frente a qué tipo de información o documentos pueden establecerse restricciones al derecho de acceso de información pública, la terminología elegida no se opone a nuestro ordenamiento, y de hecho es compatible con el lenguaje empleado en otras leyes estatutarias sobre el derecho al habeas data.

56. Los algoritmos han pasado a definir buena parte de nuestras vidas. Ellos determinan aspectos de nuestra cotidianidad, como las canciones que oímos, la publicidad comercial a la que estamos expuestos o las rutas que tomamos para ir al trabajo. Sin embargo, los algoritmos también juegan un rol cada vez más importante en la relación con el Estado y en la definición de las políticas públicas. En la actualidad, los algoritmos intervienen en decisiones tales como a quién se le otorga un subsidio o un cupo en una escuela o universidad pública, dónde se ubica una guardería, a quién se le otorga o niega una visa, o cuál es la mejor medida de aseguramiento o pena para una persona, según sus antecedentes. En otros términos, la existencia y uso de algoritmos por parte de la administración pública tiene implicaciones claras sobre los derechos de las personas. Uno de los derechos que se puede ver afectado por el uso cada vez más común de algoritmos para la toma de decisiones por parte de entidades públicas es el derecho de acceso a la información.

57. Pero ¿qué es un algoritmo? Él puede definirse como el conjunto de reglas y procedimientos que se siguen para resolver un problema determinado de manera lógica y eficiente[97]. En palabras más sencillas, un algoritmo es una serie de pasos ordenados que hacen que una información de entrada -"input"- se convierta en un resultado –"output", y puede ser implementado en forma de un programa de computación que resuelve el problema de forma automatizada y mucho más veloz. Sin embargo, para que un computador tenga la capacidad de entender y procesar un algoritmo, este debe ser traducido a un lenguaje computacional. Esa traducción del algoritmo es lo que se conoce como el código fuente.

58. En esencia, el código fuente es la columna vertebral del software o la aplicación, y es lo que proporciona la estructura y las directrices necesarias para que se ejecuten las instrucciones o pasos previstos en el algoritmo. Estos pasos pueden consistir en procesar datos, tomar decisiones y producir resultados. Sin esta base, el algoritmo carecería de la dirección y la lógica necesarias para operar. Esa funcionalidad del código fuente pone en evidencia

---

[97] Yanofsky, Noson S. Towards a Definition of an Algorithm. En: Journal of Logic and Computation. Volume: 21. Issue: 2, April 2011. Disponible en: https://bit.ly/3xxwKdE.

su importancia crítica en el desarrollo y funcionamiento de cualquier programa informático.

59. Existen códigos fuente abiertos y otros que no lo son. Un código abierto es un código fuente que ha sido puesto a disposición del público para que cualquiera pueda modificarlo y construir sobre él. La idea detrás del concepto es incentivar una actividad colaborativa y que los códigos tengan una mejora continua. Este tipo de códigos suelen tener una licencia abierta que puede reconocer ciertos derechos al creador original del código, en algunos casos bajo la figura de derechos de autor, pero que permite que se siga compartiendo y modificando el código libremente[98].

60. El uso de códigos abiertos ha impulsado la innovación, al permitir que desarrolladores de todo el mundo contribuyan, mejoren y adapten los softwares; también ha reducido significativamente los costos de acceso a tecnologías, pues permite, por ejemplo, que pequeñas y medianas empresas puedan acceder a softwares avanzados sin tener que hacer inversiones significativas para adquirirlos y renovarlos; también ha propiciado sistemas algorítmicos más seguros y fiables, pues al estar disponibles públicamente, permite mayores revisiones sobre el código y que se detecten o corrijan errores o fallas de forma más rápida. Por lo anterior, este modelo de colaboración global y conocimiento compartido ha revolucionado la forma en que se desarrolla, comparte y utiliza el software y la tecnología[99].

61. Sin embargo, no todos los códigos fuente son códigos abiertos. En general, se ha considerado que, al ser producciones escritas del intelecto, este tipo de creaciones se pueden proteger bajo la figura de derechos de autor, como si fueran obras literarias[100]. En ese sentido, quien tenga los derechos

---

[98] Un ejemplo de estas licencias es la Licencia Publica General de GNU (GPL GNU) que, por un lado, le da libertad al receptor final de usar el código, modificarlo y distribuirlo con los cambios, pero, por el otro lado, exige que se siga redistribuyendo el código bajo la misma licencia.

[99] Para más información sobre la evolución del código abierto, se puede consultar Stuckart, D. (2007). Open Source Software and the Invisible Revolution. En R. Carlsen, K. McFerrin, J. Price, R. Weber & D. Willis (Eds.), *Proceedings of SITE 2007--Society for Information Technology & Teacher Education International Conference* (pp. 1690-1694). San Antonio, Texas, USA: Association for the Advancement of Computing in Education (AACE)

[100] En efecto, el numeral 1º del artículo 10 del Acuerdo Sobre los Aspectos de los Derechos de Propiedad Intelectual relacionados con el Comercio (ADPIC), establece que "los programas de ordenador, sean

morales y patrimoniales sobre la obra es quien define a quién, de qué forma y bajo qué condiciones se distribuye. Así, hay empresas que deciden mantener sus códigos fuente privados porque son la base de un producto comercial que les permite diferenciarse de sus competidores (por ejemplo, el código fuente del software IOS, utilizado por los productos de Apple). También existen códigos fuente que, por el hecho de ser utilizados por entidades públicas para determinados fines, se mantienen en privado, porque su publicidad puede representar un riesgo para la seguridad nacional, aspecto sobre el cual esta sentencia ahondará más adelante.

62. Los códigos fuente son el elemento central de los sistemas de toma de decisiones automatizadas (SDA). Estos sistemas son herramientas que utilizan un proceso algorítmico para llegar a una decisión, ya sea un ranking, calificación o asociación, que puede llevar luego a otra acción o comportamiento. Se dice que estos sistemas actúan en el marco de la inteligencia artificial, o que son sistemas de inteligencia artificial, porque contribuyen a procesos de toma de decisiones que normalmente serían llevados a cabo por humanos[101]. Son este tipo de sistemas a los que se hizo referencia más arriba, en los que, con base en el algoritmo, o su traducción al código fuente, se procesa determinada información o datos (como el estado del tráfico, o las calificaciones y estatus socioeconómico de un potencial estudiante) para llegar a una decisión (la ruta más rápida o el cupo en determinada universidad), o, por lo menos, para informar o apoyar a un individuo en la toma de decisiones.

63. En ese sentido, otro elemento importante para entender la relevancia actual de los sistemas algorítmicos tanto para la administración pública como para la vida cotidiana es el fenómeno del *big data*. Este se caracteriza por la existencia de altos volúmenes de datos, de gran complejidad y variedad, que

---

programas fuente o programas objeto, serán protegidos como obras literarias en virtud del Convenio de Berna (1971)". Ello no implica, sin embargo, que los códigos fuente no puedan objeto de otras formas de protección, como el secreto empresarial o la patente. Al respecto, se puede consultar: Sarmiento Paez, C (2016). "La protección del software desde la Propiedad Intelectual en Colombia: Conveniencia de la creación de una normativa especial que garantice los derechos de los desarrolladores". Sobre la discusión en torno a cuál es la mejor forma de proteger el código fuente, puede verse también: Katyal, S. (2019). "The Paradox of Source Code Secrecy", Cornell Law Review 104:5.

[101] Diakopoulos, N. (2020)."Transparency." En M. D.Dubber, F. Pasquale, & S.Das (Eds.), The OxfordHandbook of Ethics of AI.Oxford University Press.

pueden ser utilizados por los sistemas computacionales para la toma de decisiones. Así, en virtud del *big data* y gracias al aumento exponencial de la capacidad computacional, actualmente existe la posibilidad de recolectar y procesar rápidamente una cantidad masiva de información de los individuos, tanto en términos de datos personales como de sus gustos, preferencias y hábitos, para todo tipo de finalidades[102]. Esto, a su vez, ha expandido el alcance y uso de los algoritmos a casi todos los ámbitos de la vida.

64. En efecto, en los últimos años, se ha presentado un rápido avance y despliegue de sistemas algorítmicos para la toma automatizada de decisiones en sectores públicos y privados a nivel mundial. En Colombia, por ejemplo, se han adoptado al menos 111 sistemas de toma de decisiones automatizadas (SDA) en etapas de pilotaje o ejecución por entidades públicas[103]. La adopción de SDA puede generar grandes beneficios para dichas entidades y, en general, para la población, pues no solo es una forma de reducir costos, sino que puede mejorar la distribución de recursos y servicios públicos, y hacer que las decisiones de política pública sean más eficientes, confiables y precisas. Sin embargo, el uso de estas tecnologías también puede ocasionar riesgos y vulneraciones de derechos fundamentales como la no discriminación, el debido proceso y la protección de datos personales.

65. Por lo tanto, la transparencia en el uso de esta herramienta es una garantía fundamental para asegurar un empleo adecuado y razonable de los datos personales y evitar que el uso de sistemas algorítmicos para la toma de decisiones por parte de entidades públicas derive en decisiones arbitrarias o discriminatorias. Bajo esta finalidad surge el concepto de **transparencia algorítmica**, que se define como la disponibilidad de información sobre sistemas de algoritmos que permite conocer su operación y valorar su rendimiento[104]. Lo que se busca con la transparencia algorítmica es, en otros

---

[102] Urueña, R. "Autoridad algorítmica: ¿cómo empezar a pensar la protección de los derechos humanos en la era del 'big data'?" Latin American Law Review n.º 02 (2019): 99-124, doi: https://doi.org/10.29263/lar02.2019.05

[103] Gutiérrez, J.D., & Castellanos Sánchez, M. (2023) Transparencia algorítmica y Estado Abierto en Colombia. Reflexión política 25(52), p. 7. Disponible en: https://bit.ly/3Vt4pgD.

[104] La definición de transparencia algorítmica que se presenta en esta sentencia se toma de los siguientes artículos académicos: (i) Porumbesu, G., Meijer, A. & Grimmelikhuijsen, S. (2022). Government transparency:

términos, que el público en general pueda comprender cómo los sistemas de toma de decisiones automatizadas (SDA) procesan los datos que capturan y cómo toman decisiones que afectan la vida de las personas. Se trata de un principio con un fin constitucional: democratizar el funcionamiento interno de un sistema de toma de decisión automatizado, para que sea entendible por quienes se ven afectados por su puesta en marcha y operación.

66. La transparencia algorítmica es particularmente relevante en el uso de SDA por parte de entidades públicas. Lo anterior, debido a que las decisiones que toma el Estado a través de estos sistemas tienen efectos importantes en materia de derechos, incluido el derecho de acceso a la información pública, que se desarrolló ampliamente en las primeras secciones de esta sentencia.

67. En efecto, en un sistema constitucional y democrático, los ciudadanos deben conocer la forma, el fundamento y el proceso a través del cual se toman las decisiones de política pública que los afectan. Cuando los ciudadanos no conocen la forma en la que las aplicaciones o sistemas de toma de decisiones están construidas, no pueden llegar a entender a cabalidad cuál es la finalidad con la que el Estado usa los datos de las personas. Tampoco pueden saber si existen defectos en el diseño que lleguen a generar o reproducir graves discriminaciones o sesgos. Por ello, el derecho de los ciudadanos a acceder, en la medida de lo posible, a información sobre los sistemas algorítmicos que utiliza el Estado para la toma de decisiones, y el uso que se le da a los mismos, es una garantía fundamental para evitar que estas tecnologías lleven a la vulneración de otros derechos fundamentales.

68. Como se pasará a mostrar, la importancia de conocer esta información se hizo especialmente evidente en el marco de la pandemia del Covid 19, cuando varios gobiernos alrededor del mundo, incluyendo el colombiano,

---

State of the art and new perspectives. Cambridge University Press; (ii) Garrido, R., Lapostol, J. P., & Hermosilla, M. P. (2021). Transparencia algorítmica en el sector público. Escuela de Gobierno de la Universidad Adolfo Ibáñez. Disponible en: https://bit.ly/3V5Tvvj. [Consultado el 29 de julio de 2022 a las 5:45 PM]; (iii) Criado, I., Valero, J & Villodre, J. Algorithmic transparency and bureaucratic discretion: The case of SALER early warning system. Information Polity 25 (2020), pp. 449 a 470; Ada Lovelace Institute, AI Now Institute and Open Government Partership. (2021) *Algorithmic Accountability for the Public Sector.* Disponible en: https://bit.ly/3hsqprU; y Gutiérrez, J.D., & Castellanos Sánchez, M. (2023) Transparencia algorítmica y Estado Abierto en Colombia. Reflexión política 25(52), p. 7. Disponible en: https://bit.ly/3Vt4pgD. .

optaron por utilizar sistemas algorítmicos como parte del manejo epidemiológico del virus, a través del procesamiento de los datos personales de miles de ciudadanos. Pasa entonces la Corte a describir brevemente dicho uso y algunas de las medidas que se implementaron para garantizar condiciones de transparencia.

6.1. La transparencia algorítmica en el contexto de la pandemia

69. Tras la declaratoria de una pandemia mundial por el Covid 19 en marzo de 2020, surgieron diferentes tipos de aplicaciones y softwares con la finalidad de ayudar a controlar el avance del virus. Algunos gobiernos utilizaron esas tecnologías para monitorear a las personas que estaban en cuarentena utilizando los datos de ubicación de sus dispositivos. Otros desarrollaron aplicaciones para que los ciudadanos reportaran sus síntomas o para rastrear posibles contactos positivos. En general, esas aplicaciones utilizaban las señales de GPS o de bluetooth para establecer la ubicación de las personas, los contactos cercanos y evaluar los riesgos epidemiológicos. También se utilizaron para recopilar datos de las personas, algunos relacionados con su estado de salud, pero también con otros datos personales como sus direcciones de residencia, correos, datos de contacto, etc.

70. Fue en ese contexto que se creó y puso en operación la aplicación CoronApp, que se relaciona con el caso que hoy estudia la Corte. Esta era una una aplicación para teléfonos móviles que incorporaba funciones para hacer rastreo de ubicación y de contagio por proximidad. Así, al descargar la aplicación, las personas debían activar permisos para que esta pudiera acceder y transmitir periódicamente los datos de localización de la persona (del dispositivo móvil, en realidad), así como permisos para que, a través de bluetooth y wifi se pudiera rastrear el contacto con alguien que resultó positivo para el virus. Además, las personas podían reportar su estado de salud y el de su familia. En consecuencia, para el uso y funcionamiento de la aplicación se debían registrar una serie de datos personales de los usuarios que luego servían para generar alertas y llevar un control sobre el registro de contagios.

71. Aplicaciones similares a CoronApp se utilizaron en diversos países e hicieron que la discusión en torno a los impactos de la inteligencia artificial y

el uso masivo de datos personales sobre los derechos humanos cobrara especial relevancia. Si bien esas aplicaciones podían llegar a ser útiles para enfrentar o contener el contagio del virus, daban acceso a una cantidad masiva e importante de datos de las personas que podía llegar a ser utilizada para fines diferentes a los previstos y violar la intimidad y privacidad de las personas. Así, dependiendo del uso que se le diera a los datos, una aplicación para el control sanitario y epidemiológico podría utilizarse como una herramienta de vigilancia masiva por parte del Estado. Por lo tanto, más allá de los riesgos sobre el derecho al habeas data, en el marco de la pandemia y ante el aumento exponencial de este tipo de aplicaciones, se evidenció que estas aplicaciones podían tener consecuencias sobre otros derechos como la libertad de expresión, de locomoción y los derechos políticos.

72. Estas preocupaciones llevaron a que en mayo de 2020 la Organización Mundial de la Salud (OMS)[105] publicara un informe provisional sobre las consideraciones éticas a tener en cuenta en las tecnologías de rastreo por proximidad desarrolladas para el Covid-19. Algunos de los principios recogidos en el informe son los siguientes:

(i) las medidas deben ser temporales y limitadas.
(ii) Las tecnologías deben ponerse a prueba previamente, y hay que garantizar que sean robustas y no tengan fallas de seguridad. Por ende, debe haber un monitoreo constante y una evaluación pública por parte de un tercero independiente.
(iii) La recolección y procesamiento de datos debe ser proporcional, estar justificada, ser idónea, necesaria, razonable y proporcionada. Siempre se deben preferir las medidas menos intrusivas de la privacidad.
(iv) La comercialización de los datos debe estar prohibida.
(v) Se deben tomar todas las medidas de seguridad sobre los datos personales. Las aplicaciones deben ser auditadas y se deben publicar los protocolos de seguridad que existen sobre los datos.
(vi) La recolección y procesamiento de datos debe ser transparente y se debe poder explicar. A los individuos se les debe suministrar

[105] Organización Mundial de la Salud (2020). *Ethical considerations to guide the use of digital proximity tracking technologies for COVID-19 contact tracing: interim guidance*, Mayo 28, 2020. . https://iris.who.int/handle/10665/332200.

información en lenguaje claro sobre el propósito de la recolección, y la forma y tiempo en que se almacenarán y compartirán los datos. Debe haber total transparencia sobre el funcionamiento de las aplicaciones, y deben publicarse los códigos fuente.

(vii) El modelo algorítmico que se utiliza para procesar los datos y evaluar el riesgo de contagio debe estar verificado y validado por un tercero.

73. Como lo mencionaron algunos de los intervinientes en este proceso, varios Estados que decidieron utilizar tecnologías de inteligencia artificial para manejar el contagio del virus tomaron medidas de transparencia como publicar los códigos fuente de las aplicaciones o "abrirlos" para que otros pudieran modificarlos, mejorarlos y aprovecharlos para hacer su propio rastreo de contactos. Así, por ejemplo, lo hizo Alemania con la aplicación Corona-Warn-App y la India con Covid 19 Aarogya Setu. Los gobiernos de Bélgica, Eslovenia y Chipre se basaron en el código abierto de Alemania para construir sus propias aplicaciones, y también mantuvieron el código fuente abierto. Los gobiernos de Australia y Nueva Zelanda utilizaron un código abierto desarrollado por el gobierno de Singapur para crear sus propias aplicaciones, que mantuvieron con licencias abiertas[106]. Los gobiernos de Brasil y Ecuador también publicaron los códigos fuente de las aplicaciones de rastreo de contactos. En España, aunque en un principio no se publicó el código fuente de la app Radar Covid, más adelante se publicó tras la presión de la sociedad civil. En efecto, ella hizo un llamado de transparencia para garantizar un escrutinio multidisciplinar a través del cual se pudieran "identificar de forma eficiente sesgos potenciales y errores en la conceptualización e implementación de la aplicación que puedan dar lugar a efectos indeseados en términos de discriminación y vulneración de derechos"[107].

---

[106] Comisión Europea :, A., Birov, S., Wyl, V., Ebbers, W. et al., *Digital contact tracing study – Study on lessons learned, best practices and epidemiological impact of the common European approach on digital contact tracing to combat and exit the COVID-19 pandemic*, Oficina de publicaciones de la Unión Europea, 2022, https://data.europa.eu/doi/10.2759/146050

[107] Manifiesto en favor de la trasnparencia en desarrollos de softwares públicos. Disponible en: https://transparenciagov2020.github.io

74. En un estudio hecho por la Unión Europea[108] en el que se analizaron 27 aplicaciones digitales nacionales de rastreo de contactos, se constató que 25 de ellas eran de código abierto. También algunos desarrolladores privados como la empresa española Acciona crearon códigos fuente con licencia abierta y gratuita para que las empresas pudieran incorporar aplicaciones de rastreo de contagio para sus empleados.

75. En suma, ante el inmenso poder que adquirieron estas aplicaciones en medio de la urgencia, y teniendo en cuenta la cantidad y sensibilidad de los datos que manejaban, muchos gobiernos optaron no solo por publicar los códigos fuente de las aplicaciones, sino también por abrirlos al público para que otros pudieran seguir construyendo sobre los mismos y les ayudaran a identificar vulnerabilidades y oportunidades de mejoramiento. Algunos gobiernos implementaron otras medidas de transparencia, como publicar los estudios de impacto sobre el tratamiento de datos personales y llevar a cabo consultas participativas con organizaciones de la sociedad civil para garantizar que el desarrollo de las aplicaciones estuviera centrado en el individuo[109].

76. En esa medida, las aplicaciones que se desarrollaron en el contexto de la pandemia prendieron las luces sobre un tema crucial para las sociedades contemporáneas, en las que el uso de algoritmos y el flujo masivo de datos son una constante: la intersección entre la tecnología y los derechos humanos. Como se mencionó, uno de los aspectos concretos de ese debate gira en torno a la transparencia en el uso de estas tecnologías. Por ello, a continuación, la Corte ahondará en el concepto de trasparencia algorítmica y la forma en la que este se ha materializado en diferentes tipos de regulaciones alrededor del mundo.

6.3. Transparencia algorítmica. Tipologías y ejemplos de regulación

---

[108] Comisión Europea: A., Birov, S., Wyl, V., Ebbers, W. et al., *Digital contact tracing study – Study on lessons learned, best practices and epidemiological impact of the common European approach on digital contact tracing to combat and exit the COVID-19 pandemic*, Oficina de publicaciones de la Unión Europea, 2022, https://data.europa.eu/doi/10.2759/146050

[109] Esto se hizo, por ejemplo, en Irlanda del Norte. Ver: Ibidem, pág. 28.

77. Como arriba se mencionó, la transparencia algorítmica busca que la información sobre los sistemas algorítmicos de toma de decisiones esté disponible para que las personas puedan entender cómo funcionan los sistemas y valorar su rendimiento. La transparencia se contrapone, entonces, a la opacidad algorítmica o los algoritmos llamados como black box, en los que se conocen los datos de entrada y el resultado, pero no la forma en la que la información es procesada[110]. Se trata de una garantía fundamental en una sociedad democrática, pues si un sistema de toma de decisiones automatizadas (SDA) opera y toma decisiones de manera opaca, es imposible que la sociedad evalúe su capacidad de actuar con justicia y equidad, o su impacto en la autonomía y la dignidad de las personas.

78. Como su propia definición lo revela, la transparencia algorítmica es un concepto que se deriva de un elemento que hace parte sustancial e inescindible de la naturaleza del derecho fundamental al acceso a la información pública: la disponibilidad de información. A través de la transparencia algorítmica se busca que los ciudadanos puedan conocer y comprender el funcionamiento de los algoritmos con base en los cuales las entidades públicas toman decisiones que los afectan. Esto puede lograrse de diferentes maneras. Una de ellas, pero no la única, es la publicación del código fuente, que, como se vio, es el documento que hace que el algoritmo pueda operar. Sin embargo, la transparencia algorítmica también se puede garantizar dando a conocer la lógica detrás del algoritmo, su arquitectura o la información sobre cómo se recolectan, se almacenan y se procesan los datos. En ese sentido, la transparencia algorítmica debe ser vista como un espectro en el que, a través de diferentes mecanismos, se le permite a la ciudadanía conocer y entender la forma en la que los sistemas utilizados por las entidades públicas toman las decisiones[111].

79. En el marco de la transparencia algorítmica se ha diferenciado entre la transparencia perfecta o completa y la significativa. En la perfecta, el receptor de la información tiene un conocimiento completo de las reglas de

---

[110] *Black Box AI: What Is It And How Does It Work?*Diposinble en:: https://eastgate-software.com/black-box-ai-what-is-it-and-how-does-it-work/#:~:text=Black%20Box%20AI%2C%20in%20essence,explainable%2C%20even%20by%20their%20creators.

[111] Diakopoulos, N. (2020)."Transparency." En M. D.Dubber, F. Pasquale, & S.Das (Eds.), The OxfordHandbook of Ethics of AI.Oxford University Press.

funcionamiento del sistema y de su proceso de creación, mientras que en la segunda se tiene un conocimiento suficiente para valorar el algoritmo. En ese sentido, no necesariamente se requiere conocer la totalidad de la información, sino lo necesario para que las personas puedan entender y valorar el sistema algorítmico detrás de las decisiones públicas.

80. La transparencia significativa tiene dos elementos implícitos que son la accesibilidad y la explicabilidad[112]. El primero de estos elementos implica ir más allá de la mera publicidad de la información y permitir auditorías o inspecciones externas que analicen y expliquen sus impactos. Esto, pues el público general puede no entender el lenguaje técnico que se emplea en esos sistemas y, en todo caso, incluso alguien con conocimiento experto puede no prever los impactos del algoritmo. Por ejemplo, en Canadá, dependiendo del nivel de impacto de una decisión tomada con un sistema algorítmico, se deben hacer consultas previas con expertos, que pueden ser del gobierno o externos, y luego publicar sus evaluaciones en lenguaje claro[113].

81. El segundo elemento, la explicabilidad, implica que las personas deben poder entender, en lenguaje sencillo y concreto, cómo el sistema llegó a un determinado resultado. Un ejemplo de una medida de transparencia significativa, a través de la cual se busca garantizar la explicabilidad, es el Reglamento General de Protección de Datos de la Unión Europea. Allí se señala que, cuando se obtengan datos personales que van a ser objeto de tratamiento a través de un sistema de decisión automatizado, se deberá informar a la persona interesada sobre la existencia del sistema y darle información significativa sobre su lógica y sobre la importancia y las consecuencias que el tratamiento automatizado puede tener para ella[114]. En Francia, en virtud de la Ley de República Digital, se ha incentivado el uso de explicaciones en video u otros formatos más accesibles para que las personas puedan entender la lógica algorítmica detrás de un sistema de toma de

---

[112] Valderrama, M; Hermosilla, M; y Garrido, R. State of the Evidence: Algorithmic Tranparency. Universidad Adolfo Ibáñez, 2023.

[113] Directiva del gobierno canadiense para la toma de decisiones automatizada. Apéndices B y C. Dispoible en: https://www.tbs-sct.canada.ca/pol/doc-eng.aspx?id=32592

[114] Reglamento General de Protección de Datos de la Unión Europea, artículo 13.2.f. y 14.2.g.

decisiones automatizadas (SDA)[115]. En Canadá, dependiendo del impacto que pueda tener el SDA, se debe dar información sobre el papel que juega el sistema en el proceso de toma de decisiones, los datos que utiliza y cómo se recolectan, los criterios utilizados para evaluar los datos y las operaciones que se aplicaron para procesarlos, entre otras cosas[116].

82. Así, si bien no existe un estándar que defina qué tipo de información, o en qué cantidad, es necesaria para garantizar la transparencia, algunos estudios han definido diferentes dimensiones de información que se pueden dar a conocer para que haya mayor transparencia. Por ejemplo, se puede dar información sobre el nivel y la naturaleza del involucramiento humano en el desarrollo y ejecución del sistema, que responde a preguntas tales como ¿quién lo diseñó?, ¿con qué finalidad?, y ¿qué tanto intervienen los humanos en la operación y monitoreo del sistema? También se puede dar información sobre los datos usados para entrenar u operar el sistema, que responde a interrogantes relacionados con el tipo de datos que utiliza, la forma de recolección, las variables para ello, la existencia de un consentimiento previo cuando se utilizan datos personales, la forma de protección de los datos, el tiempo de almacenamiento, las clasificaciones o predicciones del modelo algorítmico, los posibles errores del sistema y la forma en la que se mitigan o remedian los errores o riesgos[117].

83. Ahora bien, otra tipología relevante es la que diferencia entre la transparencia activa y la pasiva. La activa puede surgir por un deber legal o por voluntad de la administración y es aquella en la que el Estado, de manera abierta y permanente, ofrece información sobre sus sistemas de operación a través de la publicación periódica en portales de datos abiertos o en repositorios de licencias públicas de desarrollo de aplicaciones. Se trata de una estrategia que reduce la opacidad en el desarrollo y uso de herramientas por

---

[115] Ada Lovelace Institute, AI Now Institute and Open Government Partership. (2021) *Algorithmic Accountability for the Public Sector.* Disponible en: https://bit.ly/3hsqprU, pág. 19.

[116] Directiva del gobierno canadiense para la toma de decisiones automatizada. Apéndices B y C. Dispoible en: https://www.tbs-sct.canada.ca/pol/doc-eng.aspx?id=32592

[117] Diakopoulos, N. (2020)."Transparency." En M. D.Dubber, F. Pasquale, & S.Das (Eds.), The OxfordHandbook of Ethics of AI.Oxford University Press. Citado en: Valderrama, M; Hermosilla, M; y Garrido, R. State of the Evidence: Algorithmic Tranparency. Universidad Adolfo Ibáñez, 2023.

parte del Estado. Así, en la transparencia algorítmica activa hay una acción decidida del gobierno de poner la luz sobre sus operaciones digitales.

84. Sobre la transparencia algorítmica activa se pueden dar varios ejemplos. Algunos países, ciudades o distritos exigen que el gobierno tenga un registro público de todos los SDA o de inteligencia artificial que utiliza para la toma de decisiones, de tal forma que la ciudadanía pueda saber en qué decisiones se están utilizando estas tecnologías. Un ejemplo de estos registros se puede encontrar en ciudades como Nueva York (EEUU), Helsinki (Finlandia), Ontario (Canadá), Ámsterdam (Países Bajos) o Nantes (Francia), y a nivel nacional en países como Francia o el Reino Unido[118]. En Nueva York, por ejemplo, las entidades públicas tienen la obligación de reportar todas las herramientas algorítmicas que: (i) utilicen u operen sobre sistemas complejos de análisis de datos, (ii) apoyen el proceso de toma de decisiones de las entidades, y (iii) tengan un efecto público material. En el registro se debe precisar el nombre de la herramienta algorítmica y el propósito, y explicar su funcionamiento general[119]. Algunos de estos registros o inventarios incluyen también un repositorio con el código fuente de los sistemas.

85. También existen otros mecanismos de transparencia activa basados en auditorías externas, evaluaciones o estudios de impacto. Por ejemplo, en Canadá y Uruguay se exige que quienes manejan programas de política pública que utilizan SDA lleven a cabo un estudio de impacto algorítmico antes de ponerlo en funcionamiento[120]. Estos estudios o evaluaciones también son de libre acceso. Asimismo, el recientemente aprobado Reglamento sobre Inteligencia artificial de la Unión Europea exige que las entidades públicas que vayan a hacer uso de sistemas de inteligencia artificial de alto riesgo lleven a cabo, antes de su puesta en funcionamiento, una evaluación de impacto relativa a los derechos fundamentales[121]. Si bien esta evaluación no

---

[118] Ada Lovelace Institute, AI Now Institute and Open Government Partership. (2021) *Algorithmic Accountability for the Public Sector.* Disponible en: https://bit.ly/3hsqprU, pág. 19.

[119] Disponible en: https://www.nyc.gov/assets/oti/downloads/pdf/reports/ampo-agency-compliance-cy-2020.pdf

[120] https://www.tbs-sct.canada.ca/pol/doc-eng.aspx?id=32592

[121] Reglamento de Inteligencia Artificial del Parlamento Europeo. Artículo 27.

necesariamente es pública, es una medida de transparencia activa que puede minimizar el impacto del uso de estas tecnologías sobre los derechos.

86. La transparencia pasiva, por el otro lado, es aquella que se da a raíz de solicitudes de acceso a la información. En estos casos, el Estado publica información sobre el algoritmo o sobre el SDA que utiliza en sus procesos, como respuesta a solicitudes específicas elevadas por cualquier ciudadano en ejercicio de su derecho de acceso a la información pública.

87. En este punto, es necesario hacer un paréntesis importante, pues parte de la discusión que plantea el presente caso gira en torno a si los sistemas algorítmicos que utilizan las entidades públicas pueden ser catalogados como documentos públicos que pueden ser solicitados por los ciudadanos en el marco del derecho al acceso a la información pública. Si bien no existe un marco vinculante en ese sentido ni una posición unificada en términos jurisprudenciales, sí hay una tendencia en el ámbito comparado de considerar que el código fuente y los tratamientos algorítmicos que usan las aplicaciones informáticas de las entidades públicas constituyen documentos públicos a los cuales se debería, en principio y por regla general, conceder acceso[122].

88. Así, por ejemplo, desde 2016, con la promulgación de la Ley de la Republica Digital en Francia, ese país reconoció el código fuente como un documento administrativo. Siguiendo esa línea, la Comisión de Acceso a los Documentos Administrativos de Francia (CADA) "ha calificado como documentos administrativos no sólo el código fuente o los algoritmos implementados por una Administración[123], sino también la documentación técnica relativa al código fuente, como puede ser el documento de

---

[122] Gutiérrez David, M.E. (2021). Administraciones inteligentes y acceso al código fuente y los algoritmos públicos. Conjurando riesgos de cajas negras decisionales, *Derecom*, 30, 143-228, http://www.derecom.com/derecom/

[123] En sentido estimatorio, CADA. Opiniones núms. 20182093, de 6 de septiembre de 2018; 20182120, de 6 de septiembre de 2018; 20182455, de 6 de septiembre de 2018; 20173235, de 30 de noviembre de 2017; 20163835, de 6 de octubre de 2016; 20161990, de 23 de junio de 2016; 20161989, de 23 de junio de 2016; en sentido desestimatorio, 20201743, de 10 de septiembre de 2020; 20184400, de 10 de enero de 2019.

especificación de requisitos de software[124]". En España, la Comisión Catalana de Garantías de Acceso a la Información Pública[125] ha señalado que el concepto de información pública debe trascender la noción tradicional de documentos y equipararse más al concepto de conocimiento, de tal forma que el derecho de acceso se pueda proyectar no solo sobre los documentos en poder de la administración, sino también sobre otros "soportes de conocimiento" que también tienen las entidades públicas, como pueden ser las bases de datos informáticas y los algoritmos[126]. Sin embargo, otras regulaciones, como el Reglamento de Inteligencia Artificial de la Unión Europea, protegen la confidencialidad del código fuente y únicamente exigen que este se ponga a disposición de una autoridad de vigilancia en ciertos casos.

89. En esa medida, si bien se trata de un debate que aún está abierto, lo cierto es que el derecho de acceso a la información pública es un derecho expansivo en el marco del cual se deben privilegiar la publicidad y la transparencia de las actuaciones públicas. El aumento exponencial del uso de sistemas algorítmicos para la toma de decisiones por parte de entidades públicas, que tienen un impacto claro y directo sobre los derechos de los individuos y determinan en gran medida su relación con la administración, hace que la noción de documento público, y el derecho de acceso que se deriva de la misma, deba ampliarse. En el contexto actual, en el que el Estado actúa no solo a través de documentos tradicionales sino con base en sistemas computacionales, el acceso a la información que maneja el Estado debe trascender las nuevas y flexibles fronteras digitales. Una visión amplia del derecho fundamental de acceso a la información pública, más acorde con la nueva forma de actuar del Estado, fomentaría una cultura de apertura y participación ciudadana, permitiendo que la sociedad civil, los académicos y otros actores interesados puedan evaluar, cuestionar y contribuir a la mejora de estos sistemas.

---

[124] CADA. Opiniones núms. 20184400, de 10 de enero de 2019; 20182093, de 06 de septiembre de 2018; 20182120 y 20182455, de 6 de septiembre de 2018, respectivamente.

[125] GAIP. Resolución 93/2019, de 22 de febrero, FJ 3.

[126] Gutiérrez David, M.E. (2021). Administraciones inteligentes y acceso al código fuente y los algoritmos públicos. Conjurando riesgos de cajas negras decisionales, *Derecom*, 30, 143-228, http://www.derecom.com/derecom/

90. Lo anterior no implica, necesariamente, que siempre y en todos los casos se deban publicar la totalidad de elementos de un sistema algorítmico, o que deba siempre publicarse y abrir el código fuente de las aplicaciones y softwares del Estado. Como se ha señalado en esta ponencia, el derecho al acceso a la información pública no es un derecho absoluto y hay limitaciones que se justifican o resultan razonables. En esa medida, la transparencia algorítmica tiene también limitaciones. En efecto, en la mayoría de las reglamentaciones relacionadas con la transparencia algorítmica, los mecanismos de transparencia incluyen excepciones relacionadas con la posible tensión que la publicidad puede generar en otros derechos o intereses, como los relacionados con la privacidad de las personas o asuntos de seguridad [127].

91. Sin embargo, en los casos en los que otros derechos entran en tensión, es posible adoptar mecanismos para evitar la opacidad. Por ejemplo, en Francia se concedió acceso a un programa informático, pero se permitió la eliminación previa de aquellas partes que pudieran verse afectadas por el secreto en materia industrial o comercial[128]. La legislación de ese país también estableció que el acceso al código fuente, o al algoritmo subyacente, está condicionado a que la administración tenga sus derechos de propiedad intelectual. En Italia, por ejemplo, se ha garantizado el acceso al software y al algoritmo subyacente, con la condición de que se respeten los derechos de propiedad intelectual y no se reproduzca el software con fines económicos[129]. En general, cuando las solicitudes de acceso generan tensión con otros derechos, se ha optado por un acceso condicionado.

92. Así pues, si bien en algunas circunstancias la afectación de otros derechos, intereses y principios, como la seguridad nacional, los datos personales o la propiedad intelectual, pueden llevar a que se niegue el acceso a elementos específicos del sistema, como el código fuente, esto no debe

---

[127] Ada Lovelace Institute, AI Now Institute and Open Government Partership. (2021) *Algorithmic Accountability for the Public Sector.* Disponible en: https://bit.ly/3hsqprU, pág. 19.

[128] CADA. Opinión núm. 20142953, de 16 de octubre de 2014

[129] Gutiérrez David, M.E. (2021). Administraciones inteligentes y acceso al código fuente y los algoritmos públicos. Conjurando riesgos de cajas negras decisionales, *Derecom*, 30, 143-228, http://www.derecom.com/derecom/, pág. 173

traducirse en una negación del derecho de acceso a la información pública, pues el Estado puede adoptar medidas que maximicen la protección de los derechos en tensión. Así, por ejemplo, previo a la remisión de la información solicitada, el Estado puede requerir que el ciudadano solicitante suscriba un formato de responsabilidad en el que se comprometa de manera clara y expresa a no utilizar la información con fines comerciales y de lucro bajo el riesgo de percibir las sanciones legales y penales por la infracción de los derechos de autor. Incluso, como una regla de trazabilidad para mantener el registro de las personas que tengan acceso al código fuente, es posible que se imponga un deber de informar al sujeto obligado, en los términos de la Ley 1712 de 2014, si el algoritmo será compartido con un tercero y con qué fines.

93. En todo caso, la Corte considera de la mayor importancia que cuando las entidades públicas o que prestan servicios públicos vayan a utilizar sistemas de toma automatizada de decisiones, o de algún tipo de inteligencia artificial, se tenga en cuenta la transparencia desde el diseño de la herramienta. Así, desde un principio estaría claro cuáles serían los riesgos de compartir determinada información y cómo se podrían minimizar, sin llevar a la opacidad. Como señaló la Corte al estudiar el uso de inteligencia artificial en la administración de justicia, es necesario que el Estado priorice herramientas que permitan materializar el mandato de transparencia en la utilización de estas tecnologías, por sobre aquellas que no permitan conocer con certeza y claridad su forma de funcionamiento.

94. En suma, como puede apreciarse, la transparencia algorítmica se puede materializar en diferentes niveles y de diferentes formas, y no siempre tiene el mismo alcance. Una transparencia significativa y útil no siempre implica una transparencia total y completa. No obstante, existe cierto consenso en torno a que la publicación del código fuente es una buena práctica de transparencia que tiene varios beneficios[130]. Al conocer cómo un algoritmo toma decisiones, no solo se crea mayor confianza en los modelos y en la responsabilidad de la administración, sino que también pueden verificarse los posibles sesgos o arbitrariedades del sistema.

---

[130] Ada Lovelace Institute, AI Now Institute and Open Government Partership. (2021) *Algorithmic Accountability for the Public Sector.* Disponible en: https://bit.ly/3hsqprU

95. Por ello, por ejemplo, la propuesta normativa hecha por el Instituto Europeo de Derecho (ELI por sus siglas en inglés) para reglamentar el estudio de impacto de los sistemas de toma de decisiones algorítmicos en la administración pública señala que las entidades que operen el sistema algorítmico deben incluir, en el estudio de impacto, el proceso para acceder al código fuente y las bases de datos con las que se entrenó el sistema. Sin embargo, también aclaran que el acceso al código y a esos datos se puede restringir totalmente o limitar cuando sea necesario para salvaguardar los intereses y derechos legítimos de quien ejecuta el sistema, del proveedor del mismo o de terceros[131]. En esa misma línea, la Ley de República Digital francesa exige que las agencias del sector público publiquen, en un formato abierto y fácil de reutilizar, las reglas que definen el algoritmo utilizado para tomar decisiones, cuando estas afecten a individuos particulares. Eso ha hecho que, por ejemplo, se publiquen los códigos fuente que se utilizan para calcular impuestos. En Canadá también se exige la publicación del código fuente con algunas excepciones de confidencialidad[132].

96. Esa postura, que aboga por la mayor transparencia posible en el uso de este tipo de herramientas, también ha sido reconocida en instrumentos de derecho blando a los que ha adherido el Estado colombiano. Si bien hasta el momento no existe una regulación nacional vinculante sobre el uso de estas herramientas tecnológicas en la gestión pública y los deberes de transparencia que se derivan del mismo, sí hay compromisos del Estado en ese sentido. Por ejemplo, en las Recomendaciones del Consejo de la OCDE sobre la Inteligencia Artificial[133], a las que el Estado colombiano adhirió, se establece la transparencia como principio y se indica que se debe proporcionar información significativa para, entre otras cosas, fomentar una comprensión general de los sistemas de inteligencia artificial. Agrega que cuando sea posible y útil, se proporcione información clara y fácil de entender sobre la

---

[131] EUROPEAN LAW INSTITUTE (ELI), 2022. *Model Rules on Impact Assessment of Algorithmic Decision-Making Systems Used by Public Administration*, European Law Institute, Universidad de Viena. Disponible en: https://acortar.link/46WRX6

[132] Ada Lovelace Institute, AI Now Institute and Open Government Partership. (2021) *Algorithmic Accountability for the Public Sector.* Disponible en: https://bit.ly/3hsqprU

[133] OECD *Legal Instruments*. *Recommendation of the Council on Artificial Intelligence*. Disponible en https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449.

fuente, el proceso y la lógica que llevaron a una decisión, de tal forma que los afectados entiendan cómo se llegó a determinado resultado.

97. En sentido similar, la Recomendación sobre la ética de la inteligencia artificial, emitida por la Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura (UNESCO)[134], también aprobada por Colombia, incluye la trasparencia como uno de los principios orientadores. Al respecto, el documento señala que se debe hacer todo lo posible por aumentar la transparencia y explicabilidad de los sistemas de inteligencia artificial, pero sin dejar de lado otros principios como la privacidad, la seguridad y la protección. Así, la transparencia permite que las personas comprendan cómo se implementan los sistemas y puede proporcionar información sobre los factores que inciden en la decisión. Además, la recomendación señala que, "[e]n los casos de amenazas graves con repercusiones adversas para los derechos humanos, la transparencia puede requerir también que se compartan códigos o conjuntos de datos"[135] y, en todo caso, invita a los Estados Miembro a que revisen sus políticas y marcos reguladores, especialmente en lo que respecta al acceso a la información, para promover mecanismos como repositorios abiertos de datos y códigos fuente públicos[136].

98. En consecuencia, la publicidad del código fuente, total o condicionada, es una de las formas en las que se puede garantizar la transparencia. Sin embargo, como pone en evidencia el presente caso, la publicidad del código fuente no está exenta de riesgos y dificultades. La Sala ahondará en algunas de ellas, por su relevancia para el caso.

6.4. Publicidad del código fuente: riesgos, retos y dificultades.

99. Una de las principales preocupaciones de transparentar el código fuente es que terceros puedan manipularlo y alterar estratégica o engañosamente su comportamiento para modificar el resultado esperado. Este es el fenómeno

---

[134] UNESCO (2022). Recomendación sobre la ética de la inteligencia artificial. Disponible en: https://www.unesco.org/es/articles/recomendacion-sobre-la-etica-de-la-inteligencia-artificial URL 3/02/2023.

[135] Ibidem, pág. 23.

[136] Ibidem, pág. 30.

conocido como *gaming* y es un argumento común que utilizan las administraciones para mantener sus sistemas algorítmicos en secreto. Sin embargo, si bien se trata de un riesgo cierto, si el sistema es lo suficientemente robusto no debería ser una preocupación[137]. Incluso, el hecho de que los ciudadanos sepan cómo funciona el sistema les permite conocer los criterios que subyacen al algoritmo y generar comportamientos virtuosos. Por ejemplo, una persona que conoce que el sistema a través del cual un algoritmo toma decisiones crediticias da un mayor puntaje a quienes pagan impuestos de manera oportuna puede empezar a hacerlo para obtener los beneficios del algoritmo. Es decir, el conocimiento sobre la función del algoritmo genera efectos sociales positivos. En todo caso, las vulnerabilidades que pueden llegar a exponer a un sistema a manipulación o engaño se pueden prever desde el diseño del modelo, incluso anticipar los posibles riesgos ante los requerimientos de transparencia del modelo.

100. Dado que los SDA manejan y funcionan sobre una gran cantidad de datos personales, otra de las preocupaciones de transparentar el código fuente gira en torno a la privacidad de esos datos. Como pusieron de presente los intervinientes en la revisión de esta acción de tutela, en general los datos que procesan los sistemas de toma de decisiones automatizadas (SDA) son un elemento aparte del código fuente y pueden analizarse de manera independiente, de tal forma que, si los SDA incorporan medidas de seguridad rigurosas para esos datos, no habría lugar a que la publicidad del código derive en un riesgo de seguridad de los datos. Sin embargo, puede ocurrir que, en virtud de la transparencia algorítmica, se compartan otros elementos de las aplicaciones o los sistemas, como códigos de acceso, contraseñas u otra información metodológica que permita, por ejemplo, desanonimizar las bases de datos y acceder a la información de los usuarios. Por ello, algunas políticas de transparencia se moderan o limitan por preocupaciones de seguridad de los datos. No obstante, los riesgos para los datos personales no siempre se derivan de la publicación del código fuente, sino también de las vulnerabilidades del sistema o aplicación como un todo.

101. Otra dificultad que se puede presentar para la transparencia del código fuente es que los algoritmos cambian y evolucionan constantemente. Este

---

[137] Cofone, I.; Strandburg, K (2019). *Stategic games and algorithmic secrecy*. McGill Law Journal, 64:4.

dinamismo lleva a que surjan dudas en torno a la transparencia, pues no resulta tan claro en qué momento, con qué frecuencia o cuál versión de la información se debe publicar. Frente a este reto, algunos recomiendan publicar las diferentes versiones, explicar los cambios entre una y otra, y aclarar cuáles son las versiones que aún son operativas[138]. En todo caso, debe recordarse que es mejor priorizar una transparencia significativa que negar el acceso en procura de una transparencia total y perfecta.

102. Finalmente, está la problemática relacionada con la competencia, los secretos empresariales y otros derechos de propiedad intelectual. En algunos casos, la transparencia total del código fuente puede generar una desventaja competitiva para un actor, pues da a conocer información que lo diferencia en el mercado y que sus competidores podrían replicar fácilmente. En efecto, los softwares y su código fuente pueden llegar a ser protegidos mediante la figura del secreto empresarial, si se cumple con los requisitos para ello. No obstante, es necesario recordar que la transparencia no es un asunto de todo o nada y que ante este tipo de dificultades ya se han previsto soluciones, en las que se hace un balance entre la protección de los intereses privados y la garantía de transparencia, siempre buscando evitar la opacidad. Por ejemplo, la normativa canadiense indica que los softwares de SDA que son de propiedad privada y toman decisiones administrativas no tienen que ser públicamente compartidos, pero sí deben ser puestos a disposición del gobierno, que retiene la facultad de inspeccionarlos y auditarlos (directamente o a través de terceros). En todo caso, deben dar una explicación significativa al público general del sistema y su funcionamiento. De manera que, si bien se protegen los derechos de propiedad intelectual asociados al software se establecen medidas de transparencia mediante la auditoría del Estado y la explicación significativa a los ciudadanos.

103. En cuanto a los derechos de autor, también existe la posibilidad de condicionar el acceso al código sin afectarlos de forma desproporcionada. Así, por ejemplo, si una entidad pública utiliza un software de un proveedor privado, puede estipular en el contrato que algunas partes del mismo serán puestas a disposición de terceros para garantizar el derecho de acceso a la

---

[138] Diakopoulos, N. (2020)."Transparency." En M. D.Dubber, F. Pasquale, & S.Das (Eds.), The OxfordHandbook of Ethics of AI.Oxford University Press

información pública condicionando dicho acceso a que el material no se utilice con fines comerciales ni se comparta con terceros.

104. En suma, aunque la publicación del código fuente es uno de los mecanismos a través de los cuales se puede garantizar la transparencia algorítmica, es claro que presenta complejidades. Habrá situaciones en que una explicación significativa sobre el funcionamiento del sistema sea más apropiada que la publicidad total del código fuente, ya que esta puede crear riesgos desproporcionados para la seguridad nacional, o desconocer secretos empresariales. No obstante, es fundamental tener en cuenta que cuando se trata de SDA a cargo de entidades públicas, la transparencia algorítmica activa y pasiva debe guiarse bajo un principio de divulgación máxima. Según este principio, es fundamental que la información revelada al público para vigilar la acción digital del Estado permita examinar el desempeño de la aplicación informática o herramienta tecnológica utilizada. Por ello, en cada caso, habrá que analizar cuál es la medida que maximiza el acceso a la información, sin afectar de manera desproporcionada otros derechos e intereses.

7. Análisis del caso concreto

105. El recorrido efectuado en esta ponencia sobre los estándares relacionados con el derecho fundamental al acceso a la información pública evidencia una constante transformación vinculada a la evolución de la sociedad y de la acción del Estado. Ante los rápidos desarrollos tecnológicos, esta relación se manifiesta en la creciente capacidad del Estado para recolectar y almacenar información del ciudadano, regular nuestras vidas y acceder a ámbitos que hace unos años parecían impensables. Por esta razón, la transparencia algorítmica se ha convertido en un elemento esencial para garantizar el derecho de acceso a la información pública. Sin embargo, como también se ha indicado, no se trata de un derecho absoluto y, por ende, en cada caso se deben analizar los derechos en tensión, la razonabilidad y la proporcionalidad de las medidas que lo limitan. Sobre esa base, la Corte entrará a analizar puntualmente la presente acción de tutela.

106. En el asunto bajo examen, la Sala revisa la acción de tutela que presentó el ciudadano Juan Carlos Upegui Mejía en contra de la Agencia Nacional Digital (AND), proceso en el que se vinculó al Instituto Nacional de Salud (INS) y al Ministerio de Salud y Protección Social. El actor sostuvo que las autoridades accionadas desconocieron su derecho fundamental al acceso a la información pública al negar la publicación del código fuente de la aplicación informática CoronApp invocando la existencia de reserva legal. Para justificar esta decisión, la agencia accionada presentó tres argumentos: el primero, relacionado con el riesgo para los datos personales que manejaba la aplicación; el segundo, con el riesgo que puede suponer la publicación del código para la salud pública; y el tercero, relacionado con los derechos de autor. Por su parte, los jueces de instancia no concedieron el amparo solicitado al considerar que las entidades accionadas negaron el acceso a la información del código fuente con la debida justificación.

107. Con base en esta controversia, la Sala debe determinar si la decisión de negar el acceso a la información del código fuente de la aplicación CoronApp vulneró el derecho fundamental al acceso a la información pública del accionante. Para resolver el problema jurídico que plantea el caso, la Sala, en primer lugar, examinará las razones expuestas por la AND para verificar si su respuesta cumplió los estándares constitucionales y estatutarios en materia del derecho al acceso a la información pública, particularmente la carga argumentativa y probatoria que se exige para negar la publicación de la información considerada de interés público. Luego, revisará la respuesta de los jueces de tutela frente a la solicitud de amparo, teniendo en cuenta que, en este caso particular, en virtud de las disposiciones estatutarias en la materia (parágrafo del artículo 27, Ley 1712 de 2014), actúan como jueces garantes del derecho al acceso a la información pública. Por último, la Sala hará unas consideraciones finales sobre la necesidad de incorporar un enfoque de máxima divulgación y proactividad algorítmica que debe orientar la acción del Estado en esta materia.

El examen de las razones expuestas por la AND para denegar el acceso al código fuente de la aplicación CoronApp

108. Lo primero que hay que indicar es que el actor es titular del derecho fundamental al acceso a la información pública y las autoridades accionadas son sujetos obligados por tratarse de entidades públicas[139]. Como se expuso en los apartados precedentes, para que un sujeto obligado pueda negar el acceso a información pública por considerar que tiene carácter de clasificada o reservada debe demostrar que: (i) la información se relaciona con un objetivo legítimo establecido legal o constitucionalmente; (ii) se trata de una de las excepciones expresamente establecidas en los artículos 18 y 19 de la Ley 1712 de 2014; y (iii) al revelar la información se causaría un daño presente, probable y específico sobre un bien o interés constitucional. Asimismo, debe demostrar en una evaluación de proporcionalidad que el daño al interés constitucional excede el interés público que representa el acceso a la información[140].

109. Igualmente, las autoridades obligadas deben observar los lineamientos que ha establecido la ley estatutaria de transparencia y del derecho de acceso a la información pública, y la jurisprudencia constitucional, cuando se invocan excepciones al acceso a la información[141]. En particular, al resolver solicitudes de acceso a la información pública deben considerar que: (i) las restricciones al derecho fundamental al acceso a la información pública son de carácter excepcional y de interpretación restrictiva; y (ii) las dudas sobre la excepción de acceso a la información de acceso deben resolverse en favor del principio de máxima divulgación. De manera que, si no se cumplen con las condiciones para negar el acceso a la información solicitada, los sujetos obligados deben acceder a publicarla.

110. De forma preliminar, para el examen que le corresponde adelantar a la Sala, debe tenerse en cuenta que, el código fuente solicitado puede ser considerado como información pública y, hasta el momento, en el ordenamiento jurídico colombiano no existe una prohibición expresa sobre la publicación de códigos fuente de sistemas algorítmicos que utiliza el Estado.

---

[139] En virtud de lo dispuesto en el literal a) del artículo 5 de la Ley 1712 de 2014.

[140] Cfr. Sentencias C-491 de 2007 y C-274 de 2013.

[141] Supra, "3.2. Marco normativo y jurisprudencial del derecho al acceso a la información pública en Colombia."

Sin embargo, como también se indicó, el derecho al acceso a la información pública no es un derecho absoluto, pues en ocasiones se justifican las restricciones. En consecuencia, esta calificación no implica por sí misma una regla de acceso ilimitado a todos los códigos fuente de las aplicaciones del Estado, pues hay eventos en los que son legítimas las restricciones de acceso, aunque, como se explicó, también proceden medidas que permitan la publicación suficiente, pero no total, u otro tipo de medidas que atiendan a la ponderación de los bienes en tensión.

111. Con base en estos presupuestos, se analizará la respuesta de la AND a la luz de los requisitos jurisprudenciales y estatutarios sobre el derecho de acceso a la información pública.

(i) La restricción se relaciona con un objetivo legítimo establecido legal o constitucionalmente

112. Primero, la respuesta de la entidad cumplió con el requisito de que la restricción elevada esté relacionada con un objeto constitucional y legalmente legítimo. Esto, por cuanto en la respuesta a la petición inicial y al recurso de reposición la AND sustentó la reserva en que existe un alto nivel de sensibilidad en la información recolectada a través de la aplicación CoronApp[142]. En ese sentido, la agencia indicó que "dentro del uso y funcionamiento de la aplicación se registran una gran serie de datos personales por parte de los usuarios de la app" [143]. Asimismo, precisó que esta

[142] Cfr. Expediente digital T-8202533. Respuesta al derecho de petición AND-EXT-00345 de 14 de octubre de 2020. En su respuesta, la AND informó que: (…) considerando el nivel de sensibilidad de la información recolectada a través de CoronApp, se decidió mantener el código en reserva hasta tanto no se cuente con el código definitivo, pues se considera que el nivel de sensibilidad de la información que se maneja en la aplicación corre riesgos al publicarlo, al tenor de lo dispuesto en el artículo 24 de la 1755 de 2015 (…) Al respecto encontramos pertinente hacer énfasis en que una vez se logre la versión definitiva el código será publicado y en que esta decisión responde únicamente a la necesidad de salvaguardar los datos personales de más de 10 millones de personas registradas en CoronApp en el marco de una pandemia que ha alterado en forma sustancial las dinámicas de la sociedad actual".

[143] Cfr. Expediente digital T-8202533. Respuesta al derecho de petición AND-EXT-00369 de 6 de noviembre de 2020. En concreto, la agencia le indicó al actor que. Dentro del uso y funcionamiento de la aplicación se registran una gran serie de datos personales por parte de los usuarios de la app con el fin de generar las alarmas de alerta y poder llevar un control sobre el registro de contagios en el territorio Nacional. Esta información recolectada a través de CoronApp Colombia es tratada únicamente para la mitigación de la emergencia ocasionada por el COVID-19, contemplando todas las medidas de protección y seguridad de la

información recaudada tiene el "fin de generar las alarmas de alerta y poder llevar un control sobre el registro de contagios en el territorio Nacional". Finalmente, como complemento, señaló que no era propietaria de los derechos de autor de la aplicación, pues los mismos se encontraban en cabeza del Instituto Nacional de Salud[144].

113. A pesar de que la entidad accionada no lo señaló expresamente, todas estas motivaciones responden a objetivos que son constitucional y legalmente legítimos. Así, el primer motivo invocado tiene como objetivo salvaguardar la información personal y el derecho a la intimidad de las personas que registraron su información en la aplicación. Se trata de la protección de un bien constitucional previsto en el artículo 15 superior, el cual dispone 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"[145] . Asimismo, la Ley 1581 de 2012 regula la protección del habeas data y precisa que el tratamiento de los datos personales registrados en cualquier base de datos sólo podrá hacerse por personas autorizadas por el titular y/o por las personas previstas en dicha ley.

114. Adicionalmente, la entidad aludió a la "vigilancia en salud pública y el despliegue de medidas en las diferentes etapas para afrontar el COVID-19", lo

---

información, de acuerdo con los principios de legalidad, finalidad, libertad, veracidad o calidad, transparencia, acceso y circulación restringida, seguridad y confidencialidad establecidos en la Ley 1581 de 2012 y en las políticas del Instituto Nacional de Salud, salvaguardando los derechos de los usuarios de la aplicación. En ningún caso se tratará la información para finalidades distintas. La aplicación CoronApp hace uso de la información con estricto cumplimiento a las normas y protocolos de Habeas Data. En tal sentido, la información recolectada a través de CoronApp Colombia es tratada únicamente para vigilancia en salud pública y el despliegue de medidas en las diferentes etapas para afrontar el COVID-19 y permitir al usuario el ingreso y uso de las funcionalidades de la aplicación.

[144] Cfr. Expediente digital T-8202533. Respuesta al derecho de petición AND-EXT-00369 de 6 de noviembre de 2020. Frente a este punto particular la AND señaló que: [r]especto de la versión iOS [de CoronApp], es importante señalar que la Corporación Agencia Nacional de Gobierno Digital, entidad encargada del desarrollo y mejoramiento continuo de la App, desarrolló integralmente dicha versión sin implementar la licencia GNU-GPL 3.0, en virtud del memorando de entendimiento suscrito con el Instituto Nacional de Salud el pasado 6 de marzo. En este sentido, al encontrarse radicados en estas entidades los derechos de autor sobre el software, se tomó la decisión de no publicar el código.

[145] Constitución Política. Artículo 15.

que responde al cuidado de la salud pública, que es un mandato constitucional consagrado en el artículo 49 superior, según el cual: "la salud y el saneamiento ambiental son servicios públicos a cargo del Estado"[146] y que este último "garantiza a todas las personas el acceso a los servicios de promoción, protección y recuperación de la salud"[147].

115. Finalmente, respecto de los presuntos derechos de autor que se pretende amparar, la Constitución señala en su artículo 61 que: "el Estado protegerá la propiedad intelectual por el tiempo y mediante las formalidades que establezca la ley"[148]. Dicho mandato constitucional tiene desarrollo legal en normas como la Ley 23 de 1982, modificada por la Ley 1450 de 2011. En consecuencia, se invoca el amparo de un bien jurídico cuya protección goza de rango constitucional y legal.

116. De manera que está acreditado el primer requisito para negar el acceso a la información pública, pues se invocó la protección de intereses y bienes constitucionales.

(ii) Se trata de una de las excepciones expresamente establecidas en los artículos 18 y 19 de la Ley 1712 de 2014

117. Segundo, pasa la Corte a evaluar si la entidad accionada identificó el fundamento legal de la reserva, particularmente si los motivos invocados corresponden a las excepciones al acceso a la información que prevé la Ley estatutaria 1712 de 2014, que corresponden a las categorías de información clasificada y reservada según los artículos 18 y 19. Sobre este requisito es necesario reiterar que la autoridad tiene la carga de identificar, de forma explícita, el fundamento legal que, en su concepto, justifica la excepción al acceso a la información pública, razón por la que no puede limitarse a plantear

---

[146] Constitución Política, artículo 49.

[147] Ibidem.

[148] Constitución Política, artículo 61.

argumentos abstractos y generales. En el presente asunto, la AND no relacionó los motivos que invocó para negar el acceso a la información con las excepciones de acceso previstas en la ley y en la Constitución. Por lo tanto, la entidad obligada incumplió la segunda de las condiciones para negar el acceso a la información pública. Este incumplimiento es suficiente para tener por acreditada la violación del derecho fundamental al acceso a la información pública por parte de la entidad accionada.

118. Sin embargo, para profundizar en el examen del asunto puesto a consideración de la Sala, se interpretarán los motivos que expuso la AND para justificar la decisión de negar la publicación del código fuente. A partir de estos elementos se puede establecer que, en principio, en lo que respecta a los argumentos relacionados, por un lado, con el derecho a la intimidad y la protección de datos personales y, por el otro, con la salud pública, podrían corresponder a las excepciones previstas en el literal a) del artículo 18 y al literal i) del artículo 19 de la Ley 1712 de 2014. Estos literales señalan, como parte de la información exceptuada del derecho de acceso a la información pública, la que ponga en riesgo el derecho a la intimidad, el derecho a la vida, la salud o la seguridad, y la que pueda poner en peligro el interés general relacionado con la salud pública.

119. En efecto, el motivo relacionado con la sensibilidad de los datos recolectados y la necesidad de proteger los datos personales de los ciudadanos registrados en CoronApp hace referencia a la causal prevista en el literal a) del artículo 18 de la Ley estatutaria 1712 de 2014. Por su parte, la razón expuesta según la cual la información está relacionada con la vigilancia epidemiológica y el despliegue de medidas efectivas para controlar la propagación del virus de la Covid 19 podría corresponder a la excepción por daño a intereses públicos prevista en el literal i) del artículo 19 de la mencionada ley estatutaria.

120. Sin embargo, con respecto al argumento relacionado con la protección de los derechos de autor que existen sobre el código fuente, la Sala no encuentra que sea uno de los motivos cobijados por las excepciones de la ley. En efecto, el literal c) del artículo 18 establece que se puede negar el acceso a la información para proteger los secretos industriales, comerciales o

profesionales. No obstante, estos no son equiparables a los derechos de autor, que son la figura a través de la cual generalmente se protegen los derechos de propiedad privados sobre los softwares y sus algoritmos subyacentes. En esa medida, si bien, como se señaló en la sección sobre transparencia algorítmica, en algunos casos resulta válido dar un acceso condicionado a códigos fuente para proteger los derechos de autor, lo cierto es que en el ordenamiento jurídico colombiano que regula el derecho fundamental al acceso a la información pública no existe una excepción con base en el potencial daño o desconocimiento de ese tipo de derechos. Al entender, según lo expuesto en esta ponencia, que el código fuente puede ser considerado información pública y que, en todo caso, los derechos de autor están en cabeza de una entidad pública, no habría razón para que, en virtud de dichos derechos, en este caso, se niegue de manera definitiva el acceso a la información.

121. Adicionalmente, debe tenerse en cuenta que una de las versiones de la aplicación, la de Android, se basó en un software de código abierto, bajo una licencia GNU-GPL. En virtud de dicha licencia, las modificaciones que se hagan a ese código abierto también deben ser públicas o accesibles a terceros, pues de lo contrario se iría en contra de la filosofía del software libre que impulsó la creación de ese tipo de licencias[149].

---

[149] Expediente digital T-8202533. Así por ejemplo, en el Amicus Curiae de la fundación Karisma, se expone que: "La propia AND afirma que CoronApp es producto de la modificación de una licencia GNU GPL-3.0, esto quiere decir que es el resultado de la modificación del software de un tercero que se encuentra, a su vez, protegido por la Licencia Pública General (GPL por sus siglas en inglés). (…) la licencia GNU GPL requiere que, quien decida modificar un software que tiene una licencia de ese tipo, debe a su vez, colocar la misma licencia a la obra que resulte de esa modificación, la premisa es que "debes dar a otros las libertades que recibes". Deber que se inspira en la filosofía del software libre, en que se fundan la licencia GNU GPL, y que afirma las cuatro libertades fundamentales de los usuarios de software libre: 1.- Ejecutar el programa 2.- Estudiar y modificar el código fuente del programa 3.- Resdistribuir copias exactas del programa y 4.- Distribuir versiones modificadas del programa. Libertades fundamentales que rigen para cualquiera que tiene acceso al software y que se materializan especialmente cuando alguien lo modifica, porque entonces pierde la libertad de definir la forma en que circulará ese software, de ahí que se obliga a que el código modificado tenga la misma licencia. Este es el caso de CoronApp, que se derivó del software de "Guardianes de la Salud" del Ministerio de Salud de Brasil y del protocolo Bluetrace de Singapur, ambos softwares licenciados con GPL versión 3.0." También, sobre este punto, como señala la intervención en sede de revisión de los docentes de la Escuela TIC del Politécnico Grancolombiano: [e]s así que la licencia GPL-3.0 garantiza la libertad para compartir y cambiar las versiones de un programa, indicando la obligación del desarrollador de "respetar las libertades de otros". Esto quiere decir que la licencia GPL no caduca y, por lo tanto, quien recibe un programa que ha sido desarrollado bajo esta licencia estaría en la obligación de compartir el código fuente con quien lo solicite. Esto debe ser así, independientemente del porcentaje de

122. En suma, dado que la posible afectación a los derechos de autor no es una de las excepciones previstas en los artículos 18 y 19 de la Ley 1712 de 2014, la Sala no analizará ese argumento.

123. Ahora bien, frente al argumento que sustenta la reserva de la información por motivos relacionados con la salud pública también es necesario hacer algunas precisiones. Como ya se indicó, el artículo 19, literal i) de la Ley 1712 de 2014 incluye la salud pública, entre otros asuntos, como uno de los motivos que podrían permitir el rechazo o denegación de solicitudes de acceso a determinada información. Sin embargo, dicho artículo también es claro en indicar que para ello el acceso debe estar "expresamente prohibido por una norma legal o constitucional". Así, por ejemplo, sucede con los documentos de los organismos de inteligencia y contrainteligencia que, en virtud del artículo 33 de la Ley 1621 de 2013[150] tienen reserva legal; o con las estrategias de defensa jurídica del Estado que, en virtud del artículo 129 de la Ley 1955 de 2019[151], son documentos reservados. Sin embargo, no ocurre lo mismo con el código fuente de CoronApp sobre el cual, hasta el momento, no existe una reserva legal expresa. En esa medida, el argumento de la AND relacionado con la salud pública no se podría enmarcar en la excepción de acceso a la información pública prevista en el artículo 19 de la Ley 1712 de 2014, pues no cumple con los requisitos necesarios que habilitan el uso de esa excepción. Por ende, la postura de la AND en lo que respecta a la salud pública no cumple con el segundo requisito que se exige para que se pueda negar el acceso. En consecuencia, la Sala no ahondará en el estudio de esa argumentación, pues no cumple con uno de los requisitos necesarios para que se pueda negar el acceso a la información.

---

código original que quede en un momento dado, pues el desarrollador aceptó las condiciones de la licencia en un principio y se benefició del trabajo de otros para iniciar su propia versión.

[150] **"Por medio de la cual se expiden normas para fortalecer el Marco Jurídico que permite a los organismos que llevan a cabo actividades de inteligencia y contrainteligencia cumplir con su misión constitucional y legal, y se dictan otras disposiciones".**

[151] "Por el cual se expide el Plan Nacional de Desarrollo 2018-2022 "Pacto por Colombia, Pacto por la Equidad".

124. En vista de lo anterior, dado que el único argumento de la AND que se puede enmarcar válidamente en una de las excepciones previstas en los artículos 18 y 19 de la Ley 1712 de 2014 es el relacionado con los datos personales y la posible afectación al derecho a la intimidad -artículo 18, literal (a) de la ley- la Sala se enfocará en su estudio. Los otros dos argumentos, relacionados con los derechos de autor y con la afectación a la salud pública, no se desarrollarán pues no se enmarcan en una de las excepciones previstas en la ley. En concreto, por un lado, porque las excepciones de acceso a la información pública no contemplan razones fundamentadas en los derechos de autor; y, por otro lado, porque no existe una disposición legal que indique que, con fundamento en la salud pública, el código fuente de aplicaciones como CoronApp tienen carácter reservado.

125. Por ello, a pesar de que la AND no identificó con claridad la excepción de acceso a la información en la que enmarcó su decisión, la Sala continuará con el análisis del argumento relacionado con los datos personales pues se trata de un tema que no ha sido abordado con anterioridad por esta corporación. Por ende, a continuación, la Sala pasará a aplicar el test del daño.

(iii) Al revelar la información se causaría un daño presente, probable y específico sobre un bien o interés constitucional

126. Para hacer este análisis, la Sala debe evaluar si la entidad accionada acreditó que la publicación del código fuente podía causar un daño **presente/real, probable y específico** en los términos del artículo 28 de la Ley 1712 de 2014 y que ese daño es de una magnitud que excede el interés público que representa el acceso a la información. Para ello, de acuerdo con las reglas estatutarias y jurisprudenciales descritas, se verificará si la entidad tuvo en cuenta la carga probatoria que exige el test de daño mencionado en los fundamentos anteriores.

127. Sobre el motivo que se examinará, la parte accionada en sus respuestas del 6 de octubre y 6 de noviembre de 2020 sostuvo que no era posible acceder a la solicitud de información, esto es, a publicar el código fuente de la

aplicación CoronApp, debido a la sensibilidad de la información recolectada a través de la aplicación y a la necesidad de salvaguardar los datos personales de un grupo considerable de ciudadanos que descargaron y accedieron a dicha herramienta[152].

128. Las razones citadas fueron los únicos elementos presentados por la parte accionada respecto a los daños que podría causar la publicación de la información y sirvieron como justificación para negar la solicitud de acceso presentada por el accionante en sede administrativa. De esta manera, la Sala procede a verificar el cumplimiento de cada uno de los elementos constitutivos del mencionado test de daño previstos en el artículo 28 de la Ley 1712 de 2014 y su decreto reglamentario.

129. *Que se trate de un daño real y presente*. El primer requisito, acreditar que el daño sea real y presente, no se cumplió. Si bien la parte accionada alegó que la versión del código fuente podía quedar expuesta a externalidades que ponían en peligro la información recolectada, lo que incluso permitiría que la aplicación pudiera ser usada de forma maliciosa o en provecho de terceros sin autorización, esas manifestaciones no explicaron en qué manera se generaría de forma inmediata y certera el daño, pues su justificación alude a una circunstancia eventual y cuya concreción, como muestra la literatura especializada, tiene baja probabilidad[153] y no se relaciona de manera directa con la publicidad del código fuente[154]. En este sentido, no basta con señalar de manera genérica un riesgo de daño, sino que es necesario demostrar que el riesgo es una circunstancia latente y próxima.

---

[152] También se alegó la protección de los derechos de autor sobre el programa, los cuales están en cabeza del INS, y razones relacionadas con la vigilancia epidemiológica y la salud pública. Sin embargo, como se explicó, estas razones resultan inadmisibles por no corresponder a alguna de las excepciones previstas en la Ley 1712 de 2014.

[153] Cofone, I.; Strandburg, K (2019). *Strategic games and algorithmic secrecy*. McGill Law Journal, 64:4.

[154] En efecto, cómo señaló la organización de Derechos Digitales, la vulnerabilidad del sistema no depende de su publicidad sino de "las defensas y mecanismos de seguridad con las que se haya dotado al programa informático, tales como la construcción por capas, el almacenamiento de las claves de acceso a la base de daros en un solo archivo, el uso de sistemas robustos para el cifrado de la información que es procesada por el programa, entre otras técnicas que los hagan resistentes a posibles ataques" (pág. 8).

130. En ese punto, es importante hacer referencia a la respuesta que la misma AND le dio a la Sala Novena al auto de pruebas de mayo del 2022. Ante la pregunta sobre las posibles medidas de mitigación del riesgo, la agencia señaló de manera clara que sí es posible desarrollar medidas que permitan garantizar la seguridad de los datos personales que se administran con una aplicación como CoronApp cuando se publica el código fuente. Dentro de esas posibles medidas, destacó la implementación de una política formal de desarrollo seguro dentro de cada entidad para regular las prácticas asociadas a la construcción, el despliegue y el mantenimiento de las herramientas informáticas que se crean y, en los casos en que se contrate con un tercero, que se establezcan una serie de exigencias contractuales en materia de seguridad y se supervise de manera directa el proceso de desarrollo de la aplicación. En consecuencia, la entidad no mostró un riesgo presente sino uno hipotético en relación con el que además aclaró que es posible contar con medidas de mitigación.

131. Además, como lo señalaron intervinientes en el proceso e incluso el perito técnico que ordenó el Tribunal Administrativo de Cundinamarca en el trámite de tutela que dio lugar a los fallos de primera y segunda instancia, los riesgos aludidos por la accionada, como suplantación de la aplicación y el denominado "phishing"[155], no requieren del código fuente, pues sin él se puede hacer igualmente una copia de la aplicación.[156] De manera que el daño alegado no resulta presente, sino remoto, eventual e indirecto.

---

[155] En la contestación de la tutela, la AND sostuvo que: "era imprudente e inoportuno publicar el código fuente de la aplicación, dado que a la fecha -de la contestación- se tenían 13'497.917 descargas y se contaba con 3'812.995 usuarios activos. De manera que constituiría un riesgo la posibilidad de una clonación (fishing) de la aplicación, que permitiera modificar funcionalidades para obtener los datos personales de los ciudadanos de forma inescrupulosa.

[156] Expediente digital T-8202533, Amicus Curiae de los de docentes de la Escuela TIC del Politécnico Grancolombiano; y dictamen pericial referido en el fallo de tutela de segunda instancia.

132. Ahora bien, la Sala tampoco encuentra probado el carácter real del daño[157], esto es, que el daño alegado se sustente en razones verídicas y no en justificaciones ajenas a la realidad.

133. Al examinar el material probatorio recaudado en el proceso, así como los conceptos de los diferentes intervinientes en sede de revisión, la Corte considera que no se acreditó que la publicación del código fuente constituyera un riesgo real frente a los intereses particulares expuestos por las autoridades accionadas.

134. En primer lugar, como se explicó, el código fuente no son los datos personales recopilados de los usuarios. La AND en sus respuestas sostuvo que la publicación del código fuente de la aplicación podría acarrear, entre otras consecuencias, que los datos sensibles de los ciudadanos quedaran expuestos a eventuales riesgos en cuanto a su tratamiento y su utilización. Sin embargo, como señalaron los intervinientes[158] y aceptaron las mismas autoridades accionadas[159], esto no es cierto, pues los datos de los usuarios deben estar almacenados de forma independiente en bases de datos que, además, deben estar cifradas y con acceso limitado por autenticación.[160] Si esta condición se cumple, entonces el código fuente por sí mismo no permite de ninguna forma que se acceda a los datos de los usuarios. De manera que el código fuente

---

[157] Pese a que el Decreto 103 de 2015 que reglamentó la Ley 1712 de 2014 establece que el daño debe ser *presente*, la sentencia C-274 de 2013 se refirió igualmente a este requisito como que el daño debe ser real.

[158] Cfr. Expediente digital T-8202533, *Amicus Curiae* de Karisma, FLIP y Derechos Digitales – América Latina, y de los docentes de la Escuela TIC del Politécnico Grancolombiano.

[159] La AND sostuvo que: "independientemente de que desde un principio se ha respetado todos los protocolos de protección de datos personales, actualmente la versión del código puede resultar expuesto a vulnerabilidades que ponen en peligro la información recolectada por la aplicación y que pone en riesgo de ser utilizada de forma maliciosa o en provecho de terceros que no sean autorizados por el Instituto Nacional de Salud."

[160] Expediente digital T-8202533, *Amicus Curiae* de los de docentes de la Escuela TIC del Politécnico Grancolombiano: "Teniendo en cuenta otras buenas prácticas como el desarrollo por capas y la descentralización, es deseable que exista en el código una separación entre la lógica de programa y las credenciales de acceso a las bases de datos donde esta información esté almacenada. Inclusive, debería haber una separación entre la lógica del programa y las direcciones de los servidores en donde se esté alojando dicha información. Asegurar esta separación evita que personal no autorizado pueda tener acceso a la información sensible que mencionan."

puede ser entregado sin que sean revelados los datos personales de los usuarios.[161]

135. De hecho, como se expuso más arriba, una de las recomendaciones de la OMS frente a este tipo de aplicaciones consistió en la publicación del código fuente. Precisamente, muchos de estos códigos se publicaron sin poner en riesgo los datos personales de los usuarios de las aplicaciones. Los casos en los que la publicidad del código fuente derivó en un riesgo para los datos personales almacenados por las aplicaciones se presentaron por errores humanos o en la arquitectura de la seguridad del sistema, mas no por la publicidad del código fuente[162].

136. En este sentido, la posibilidad de que cualquier persona estudie el código fuente no puede servir como excusa para no liberarlo. Si la aplicación cumple con estándares de seguridad y ha tenido buenas prácticas de desarrollo, como debería tener cualquier aplicación que hace un tratamiento masivo de datos personales, el análisis de dicho código no permitiría el acceso a tales datos de los usuarios. Además, la liberación del código fuente no representa un riesgo para los datos personales, ya que estos reposan en bases independientes que deberían contar con credenciales de acceso, contraseñas de seguridad y medios de autenticación que protegen su acceso.[163]

---

[161] Expediente digital T-8202533, Amicus Curiae presentado por la organización Derechos Digitales – América Latina: "Desde un punto de vista técnico, para hacer entrega del código fuente no se requiere revelar los datos personales que formen parte del mismo sistema informático, siendo posible resguardar las referencias a estos datos previo a su entrega. Por ejemplo, podría ordenarse tajar la información referida a las claves de acceso procediendo la entrega de los códigos fuente sin las claves de acceso a bases de datos." En el mismo sentido, Amicus Curiae de los de docentes de la Escuela TIC del Politécnico Grancolombiano: "el código fuente debería poderse compartir de forma segura (…) es posible compartir una versión donde las credenciales e información de acceso esté editada, borrada, anonimizada o no legible, evitando de esta forma cualquier acceso no autorizado a la información."

[162] Al respecto, ver la intervención de la Fundación Karisma, en donde se indica que las brechas de seguridad en el funcionamiento de aplicaciones móviles para el Covid 19 han sido "producto del descuido o negligencia de los responsables en la protección de la información y no han sido atribuidas en ningún caso a la publicación del código fuente" (pág. 4).

[163] Expediente digital T-8202533, Amicus Curiae de los de docentes de la Escuela TIC del Politécnico Grancolombiano. En el mismo sentido la organización Derechos Digitales – América Latina, señala en su Amicus Curiae que: "Por otra parte, puede existir preocupación por la presencia de claves o información de acceso a los sistemas con los que interactúa el programa cuyo código fuente se solicita. Pero tales claves de

137. Sobre este punto, la Corte precisa que los datos contenidos en dichas bases de datos sí corresponden a información personal[164], específicamente a información semiprivada[165] y privada[166]. Por eso, en relación con esa información, en virtud del deber de custodia que les corresponde, las entidades accionadas (artículo 2º de la Ley 1712 de 2014), como sujetos obligados, deben adelantar todas las medidas correspondientes para salvaguardarla y evitar cualquier afectación a la seguridad e integridad de esos datos. Sin embargo, se reitera que el actor, tal como señaló recurrentemente durante el trámite de la acción de tutela y en sede de revisión, no solicitó el acceso ni la publicación de este tipo de información.

138. En suma, la Sala no desconoce que existen riesgos asociados a la publicación del código fuente que pueden derivar en el acceso ilegítimo a datos personales captados por la aplicación. Sin embargo, ese riesgo: (i) no es directo, debido a la distinción entre el código fuente y los datos personales[167]; (ii) no se presenta necesariamente por el acceso al código fuente, pues estrategias maliciosas como el phishing pueden adelantarse sin el acceso a ese

---

acceso no debieran encontrarse incorporadas a este código, como también pueden retirarse del mismo previo a su entrega, a fines de descartar la potencial afectación de los derechos de las personas y al funcionamiento del organismo público."

[164] Como señaló la AND en sus respuestas a las solicitudes del actor, la aplicación recopila la siguiente información: (i) datos personales: nombre y apellido, tipo y número de documento, celular, sexo, fecha de nacimiento, país, departamento, ciudad de residencia, correo electrónico, y contraseña; (ii) datos sensibles: origen étnico, reporte de salud: estoy bien / estoy mal, síntomas, contacto con personas con síntomas, atención médica recibida, viaje a otros países.

[165] Es aquella que versa sobre información personal o impersonal y que no está comprendida dentro de la regla general de la información pública. Presenta un grado mínimo de limitación para su acceso y conocimiento. Sólo puede ser obtenida por orden de autoridad administrativa en cumplimiento de sus funciones o en el marco de los principios de la administración de datos personales. Cfr. Sentencia C-274 de 2013.

[166] Es la información que versa sobre información personal o no, que por encontrarse en un ámbito privado sólo puede ser obtenida y ofrecida por orden de autoridad judicial en el cumplimiento de sus funciones. Cfr. Sentencia C-274 de 2013.

[167] AL respecto, pueden verse las intervenciones y *amicus curiae* de la Escuela TIC del Politécnico Grancolombiano, de la Organización Derechos Digitales, de Karisma, de la FLIP, entre otros.

código[168], y (iii) el acceso indebido a los datos personales recaudados por la aplicación está más ligado a debilidades en el almacenamiento de los datos que a la publicación del código fuente[169]. A todo ello, además, se suma la respuesta de la entidad accionada que se limitó a identificar genéricamente los riesgos para negar el acceso al derecho fundamental al acceso a la información pública, sin demostrar que estos son reales y presentes.

139. En contraste, debe tenerse en cuenta que la publicación del código fuente también puede resultar beneficiosa para la seguridad de los datos, pues permitir que la población en general, así como la comunidad académica y científica en particular conozcan la forma en la que funcionan estas herramientas puede llevar a que la comunidad interesada aporte elementos de juicio a la revisión del código fuente, identificando vulnerabilidades y posibles soluciones.

140. Adicionalmente, si en gracia de discusión se admitiera que no puede separarse la información personal del código fuente bajo el principio de maximización del derecho al acceso a la información pública, la entidad debería privilegiar el acceso a la información a través de otras medidas. Así, por ejemplo, el artículo 21 de la Ley 1712 de 2014 señala que: "en aquellas circunstancias en que la totalidad de la información contenida en un documento no esté protegida por una excepción contenida en la presente ley, debe hacerse una versión pública que mantenga la reserva únicamente de la parte indispensable"[170]. De manera que los sujetos obligados debían, en última

---

[168] Expediente digital T-8202533, *Amicus Cur*iae de los de docentes de la Escuela TIC del Politécnico Grancolombiano; y dictamen pericial referido en el fallo de tutela de segunda instancia.

[169] Expediente digital T-8202533, *Amicus Curiae* presentado por la organización Derechos Digitales – América Latina: "Desde un punto de vista técnico, para hacer entrega del código fuente no se requiere revelar los datos personales que formen parte del mismo sistema informático, siendo posible resguardar las referencias a estos datos previo a su entrega. Por ejemplo, podría ordenarse tajar la información referida a las claves de acceso procediendo la entrega de los códigos fuente sin las claves de acceso a bases de datos." En el mismo sentido, *Amicus Curiae* de los de docentes de la Escuela TIC del Politécnico Grancolombiano: "el código fuente debería poderse compartir de forma segura (…) es posible compartir una versión donde las credenciales e información de acceso esté editada, borrada, anonimizada o no legible, evitando de esta forma cualquier acceso no autorizado a la información."

[170] Ley 1712 de 2014, artículo 21.

instancia, velar por cumplir con sus obligaciones, en virtud del principio de maximización de la divulgación.

141. Finalmente, ya que en las intervenciones quedó claro que no es posible hablar de una versión final o definitiva del código fuente, la entidad no podía oponerse a publicar una información bajo el argumento de que está en una etapa inacabada. En virtud de la transparencia algorítmica significativa, el derecho de acceso a la información pública se torna exigible frente a una información de calidad suficiente para que los ciudadanos puedan entender su funcionamiento y auditar su desarrollo e implementación, sin que esta información tenga que ser perfecta o completa.

142. *Que se trate de un daño probable*: en relación con el segundo requisito, esto es, que el daño sea probable, la parte accionada no señaló las circunstancias concretas que harían posible su materialización. Alegar que se corre el riesgo de que la información sea "utilizada de forma maliciosa o en provecho de terceros que no sean autorizados por el Instituto Nacional de Salud" no constituye una respuesta que satisfaga el requisito.

143. En sede de revisión las entidades accionadas, particularmente el INS, alegaron que al estar íntimamente relacionados el código fuente y las bases de datos que registran los datos personales recaudados era probable que se usara el código fuente para acceder a datos sensibles de los usuarios, lo cual afectaría diversos derechos fundamentales. Y, específicamente, señaló que era probable desarrollar una suplantación de enlaces para el ingreso a la aplicación.[171]

144. No obstante, como se señaló en el examen del requisito anterior, el eventual riesgo de la suplantación de la aplicación existe incluso sin la publicación del código fuente. Así las cosas, la Sala considera que no basta con que exista la *posibilidad* del daño, sino que este tiene que ser *probable*, es decir que exista un grado importante de probabilidad sobre la ocurrencia del

[171] Expediente digital T-8202533, intervención del INS en sede de revisión.

daño y se presenten razones y elementos suficientes que demuestren que el evento dañino podría acaecer. Igualmente, debe ser directo, esto es, debe estar relacionado con la publicación de la información requerida y no se puede invocar cualquier riesgo general.

145. Así, por ejemplo, los intervinientes y el perito técnico oficiado en el trámite de segunda instancia indicaron que, en caso de existir la posibilidad de vulnerabilidad de la información, ello sucedería por fallas en la seguridad y por malas prácticas en el desarrollo y ejecución de la aplicación. Sin embargo, este riesgo no es consecuencia de la publicación del código fuente y no se trata de razones admisibles para negar el acceso a la información pues, precisamente, les corresponde a las autoridades accionadas seguir las buenas prácticas para cumplir con el deber constitucional y legal de custodia de la información.[172]

146. *Que se trate de un daño específico:* en cuanto al presupuesto de que el daño sea específico, la parte accionada no cumplió con este requisito, pues sus razones aluden a afectaciones genéricas que no pueden individualizarse. Es decir, los argumentos de las entidades se limitan a plantear, de forma genérica, eventuales ataques de sujetos indeterminados e indeterminables.

147. Sobre este punto es importante recordar que la Corte Constitucional declaró inexequible el parágrafo 2 del artículo 5 de la Ley 1712 de 2014, que incluía una reserva ampliada sobre "información, documentos, base de datos y contratos relacionados con defensa y seguridad nacional", entre otras razones, al considerar que un "listado genérico cobija todo tipo de información, sin

[172] Expediente digital T-8202533, *Amicus Curiae* organización Derechos Digitales: "(…) conocer el código fuente de un programa no importa necesariamente que quien accede a dicha información pueda atacar y vulnerar los sistemas informáticos en que copias del mismo programa estén instaladas. La vulnerabilidad de un sistema dependerá, en definitiva, de las defensas y mecanismos de seguridad con que se haya dotado al programa informático, tales como la construcción por capas, el almacenamiento de las claves de acceso a la base de datos en un solo archivo, el uso de sistemas robustos para el cifrado de la información que es procesada por el programa, entre otras técnicas que los hagan resistentes a posibles ataques."

precisar de manera clara y concreta el tipo de información cobijada por la reserva, ni las razones por las cuales esa reserva deba garantizarse"[173].

148. Bajo este mismo entendido, la Sala considera que no es posible establecer limitaciones de confidencialidad a la información que no señalen de forma específica, esto es, clara, determinada y concreta, las afectaciones (daño) que pueda sufrir un bien jurídicamente protegido y que el sujeto obligado alega para justificar la reserva. Pues, como también lo ha señalado la Corte, frente a una circunstancia de ambigüedad, duda o vacío legal, se debe optar por una interpretación restrictiva de las excepciones al acceso a la información pública que beneficie el principio de maximización de la publicidad, razón por la que los sujetos obligados deben publicar la información solicitada.

En conclusión, la Sala constata que la parte demandada no cumplió con el deber estatutario previsto en el artículo 28 de la Ley 1712 de 2014, "**[p]or medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones",** según el cual tenía la carga argumentativa y probatoria para acreditar que, en caso de revelar la información solicitada por el actor, se causaría un daño presente/real, probable y específico sobre bienes jurídicamente protegidos.

(iv) El daño debe ser sustancial, es decir, mayor al beneficio de dar acceso a la información

149. Finalmente, además de que en el asunto bajo examen no se acreditaron los elementos constitutivos del daño, tampoco se ponderó si, al revelar la información, se excedía el interés público que representaba el acceso a la información, de manera que fuera admisible la reserva. De hecho, la entidad no explicó por qué, a la luz del interés público que supone la publicidad de la información, la reserva era la única medida idónea y necesaria para evitar el supuesto daño, ni tuvo en cuenta otras medidas menos lesivas del derecho de acceso a la información pública que hubieran podido minimizar su gravedad.

---

[173] Cfr. Corte Constitucional. Sentencia C-274 de 2013.

150. En las respuestas de la entidad tampoco se señaló el lapso concreto y las condiciones bajo las que debía permanecer la confidencialidad de la información. En este sentido, la simple y reiterada referencia de las autoridades accionadas a la constante actualización de la aplicación y la necesidad de esperar al desarrollo de un código definitivo no constituía, en ninguna manera, una justificación que acreditara este requisito. Esto debido a que el término y las condiciones que han de establecerse deben ser específicas y concretas, y no sujetas a eventos indeterminados.

151. En ese sentido, la Sala también aclara que los casos en los que se acrediten los elementos del daño (presente/real, probable y específico), la autoridad administrativa debe proceder, adicionalmente, a realizar la ponderación para determinar si la revelación de la información causaría un daño que excede el interés público que representa el acceso a la información, y a fijar de forma específica y concreta el ámbito temporal y las condiciones bajo las cuales operará la confidencialidad de la información. Esto debido a que no se puede establecer una reserva ilimitada y sin debida justificación.

152. De esta manera, al no encontrarse acreditada la carga probatoria (artículo 28 de la Ley 1712 de 2014) respecto de la configuración del daño que justificaría las excepciones al acceso a la información pública solicitada por el actor, las autoridades accionadas violaron el derecho de acceso a la información pública. Adicionalmente, se afectó el ejercicio de otros derechos. En el caso específico, la falta de transparencia y acceso al código fuente de la aplicación CoronApp privó tanto al ciudadano accionante como a la sociedad en general de la posibilidad de ejercer un control adecuado y oportuno sobre esa herramienta. Esta deficiencia no solo disminuyó la extensión, obligatoriedad y funcionalidad del derecho fundamental al acceso a la información pública, sino que también impidió que los ciudadanos pudieran verificar la precisión, seguridad y uso correcto de sus datos personales, limitando así su capacidad para proteger sus derechos a la privacidad, a la protección de datos y a la participación informada en los procesos de toma de decisiones públicas.

Los jueces constitucionales como garantes del derecho fundamental al acceso a la información pública

153. Ahora bien, establecida la violación del derecho fundamental al acceso a la información pública en el caso concreto, la Sala estima necesario hacer un pronunciamiento adicional respecto a las consideraciones expuestas por los jueces de instancia, con el fin de reiterar los deberes que constitucional y estatutariamente les corresponden a los jueces constitucionales de tutela como garantes del derecho fundamental al acceso a la información pública. En concreto, la Corte hará referencia a los deberes, herramientas y reglas relacionadas con dicho derecho que deben guiar la evaluación y ponderación, en cabeza de los jueces, y de las razones que las autoridades públicas y demás sujetos obligados invocan para sustentar excepciones de acceso a una información pública.

154. El punto de partida sobre la decisión de los jueces de tutela corresponde al reconocimiento de su papel central como garantes del derecho fundamental al acceso a la información pública, de acuerdo con la Constitución y la legislación estatutaria. Así, al examinar las razones que invocan los sujetos obligados para negar el acceso a información, los jueces deben evaluar las especiales condiciones sobre la configuración de excepciones al acceso a la información pública. Para este examen, deberán evaluar el razonamiento y la justificación expuesta por el sujeto obligado.

155. En este sentido, el juez constitucional debe determinar si el sujeto obligado cumplió con la carga argumentativa y probatoria que la Ley 1712 de 2014 impone a los sujetos obligados cuando proponen excepciones al acceso a la información pública, que se deriva del artículo 28 de la ley en mención y está resumida en esta sentencia. Asimismo, deberán guiar su examen por los principios de buena fe y por el principio de máxima divulgación. Por tanto, deben partir por entender que la reserva de información pública es excepcional, en los sujetos obligados recae la carga argumentativa y probatoria para la decisión de la limitación y, en caso de conflictos de normas, ambigüedad, falta de regulación, duda o vacío legal, debe prevalecer el derecho fundamental al acceso a la información pública.

156. Bajo esos lineamientos, es posible concluir que, en este caso, los jueces de tutela no cumplieron adecuadamente con su deber constitucional y

estatutario, especialmente en lo relativo a la verificación de las características de la argumentación desplegada por la entidad accionada sobre el daño invocado y con la valoración de la proporcionalidad de la medida. En concreto, no verificaron que se invocara un daño real y presente o probable y específico, ni evaluaron la proporcionalidad de la restricción. Finalmente, la duda invocada sobre la afectación de los intereses que buscaba proteger la reserva fue resuelta en contra del acceso a la información pública.

157. En el caso concreto, además de la falta de verificación de las condiciones del daño, los jueces de instancia sostuvieron que desde el punto de vista técnico no era suficientemente claro si la publicación del código fuente generaría eventuales riesgos de cara a la información sensible de los ciudadanos que registraron sus datos en la aplicación. Esta argumentación no constató los rasgos del daño y la proporcionalidad de la restricción del derecho de acceso a la información pública, ni aplicó la regla según la cual ante una circunstancia de duda o vacío legal respecto a las razones esgrimidas por los sujetos obligados para justificar una excepción al derecho fundamental al acceso a la información pública, debe optarse por el principio de maximización de la publicidad.

158. En este punto, se reitera que la consideración de los códigos fuentes de las aplicaciones usadas por el Estado para desarrollar sus funciones, si bien corresponden, en principio, a información pública, ello no implica una regla jurisprudencial de acceso total e irrestricto a dichos códigos. Tal y como sucede con la información pública en general, los jueces deben examinar las restricciones de acceso invocadas por las autoridades obligadas a la luz de las reglas constitucionales, estatutarias y jurisprudenciales sobre ese derecho. Dichas reglas parten de principios centrales como la buena fe y la máxima divulgación, pero también admiten restricciones excepcionales, justificadas, limitadas, proporcionales y derivadas de la ley.

159. Igualmente, en la ponderación correspondiente, inmersa en el test del daño que debe efectuar la autoridad que niega el acceso y que debe verificar la autoridad judicial, pueden explorarse otras medidas, según los bienes en tensión, como la publicidad condicionada, la eliminación de apartes que puedan significar riesgos, la elaboración de explicaciones o informes, o las

auditorías por parte de terceros; lo anterior para garantizar tanto el conocimiento general sobre cómo funcionan estos sistemas de toma de decisiones, como los derechos e intereses públicos y particulares que se pueden llegar a ver afectados por la publicidad total del código fuente. En ese sentido, ante solicitudes de información, las autoridades y los jueces constitucionales deberán analizar los riesgos y beneficios de dar acceso a determinado código fuente, así como encontrar alternativas que balanceen entre el interés público de acceder a la información y los riesgos (reales, probables y específicos) que están implícitos en esa publicidad. Priorizarán siempre la transparencia significativa y el acceso a la información.

El amparo y las órdenes tendientes a una protección integral y efectiva

160. Con base en las anteriores consideraciones la Sala revocará las decisiones de los jueces de tutela y concederá el amparo solicitado por el actor. No obstante, la Sala evidencia que algunos de las condiciones y competencias institucionales respecto de las que se debería emitir las órdenes del fallo han variado.

161. Así, por ejemplo, mediante escrito allegado por el Ministerio de Salud y Protección Social[174] dentro de los requerimientos que esta Sala ordenó en sede de revisión, informó que la titularidad de los derechos patrimoniales del autor del aplicativo CoronApp que inicialmente recaían en la AND y el INS fueron cedidos a dicho Ministerio. Explicó que el Ministerio decidió darle un nuevo alcance y uso a la aplicación, acorde con la evolución de la pandemia y el proceso de vacunación, de manera que el código fuente seguía en modificación para cumplir con las necesidades epidemiológicas. De esta manera, y debido a las nuevas funcionalidades de la aplicación, esta pasó a denominarse Minsalud Digital. Sin embargo, dicha aplicación ya no se encuentra vigente dentro del repertorio de aplicaciones móviles que maneja dicha entidad y que están disponibles para atender diferentes asuntos relacionados con la política pública en salud.

[174] Expediente digital T-8202533, intervención del Ministerio de Salud y Protección Social presentado en sede de revisión el 23 de febrero de 2022 por la Directora Técnica de la Dirección Jurídica de la entidad.

162. Con base en las anteriores circunstancias, se evidencia que el Ministerio de Salud y Protección Social, quien fue debidamente vinculado al trámite de esta acción de tutela en sede de revisión[175], es el actual sujeto obligado sobre quien reside el deber de custodia de la información solicitada por el actor. Así las cosas, la Sala ordenará a dicho Ministerio que, dentro de los 15 días siguientes a la notificación de esta decisión, entregue la información solicitada por el actor, esto es, el código fuente de la aplicación CoronApp, con todo el historial y control de versiones. Asimismo, se le ordenará que, además de darle acceso al código fuente, informe al accionante si una versión actualizada de ese código fuente se encuentra actualmente en uso en algunas de las aplicaciones de la entidad, y, de ser así, dé igualmente acceso al código fuente actualizado y en uso. Ahora bien, en caso de evidenciar que parte de ese historial se encuentra todavía en custodia de la Agencia Nacional Digital o del Instituto Nacional de Salud, el referido Ministerio deberá requerir a esas entidades que entreguen la información aquí ordenada, sin perjuicio de que el actor pueda solicitarlas directamente. En cumplimiento de lo dispuesto en esta sentencia, dichas autoridades deberán entregar la información correspondiente.

163. Asimismo, y a pesar de que no hay evidencia de ningún riesgo concreto y específico que se derive de la publicidad de la información, la Sala ordenará al Ministerio que, antes de conceder acceso al código fuente, su historial y versiones, tome, con el acompañamiento de la Agencia Nacional Digital y el Instituto Nacional de Salud, todas las medidas de seguridad necesarias para garantizar la seguridad de los datos personales de los usuarios de la aplicación. Dichas medidas pueden consistir en la creación o el fortalecimiento de contraseñas de acceso a las bases de datos, o la elaboración de una versión del código fuente en donde las credenciales o información de acceso estén editadas, borradas o anonimizadas, de tal forma que se evite cualquier acceso a esa información. Estas medidas, en todo caso, se derivan del deber de custodia que tiene la entidad sobre los datos personales, pero se deberán reforzar especialmente a la luz de la publicidad del código fuente.

---

[175] El Ministerio de Salud y Protección Social fue vinculado al trámite de la acción de tutela mediante auto del 31 de enero de 2022, proferido dentro del trámite de revisión en el proceso de la referencia.

164. En todo caso, la Sala debe aclarar que, dado que la versión iOS de la aplicación se desarrolló sin implementar la licencia GNU-GPL 3.0 (es decir, que no se construyó utilizando un software libre, sino que fue un desarrollo propio de la AND), pueden existir derechos de autor sobre esa versión del código fuente. Sin embargo, como se señaló, dichos derechos no se enmarcan en las excepciones para negar el acceso la información pública y no pueden llevar a la reserva de la misma, que es el debate constitucional central en el que se enmarca la tutela. Por lo anterior, la Corte ordenará que se garantice el acceso a ambos códigos fuente, reconociendo, en todo caso, que el titular de los derechos de autor cuenta con acciones jurídicas, diferentes a esta acción de amparo, para reclamar la protección de dichos derechos en caso de que los considere vulnerados.

165. Ahora bien, como se evidenció en la parte considerativa de esta providencia, el principio de transparencia algorítmica, en su faceta activa y pasiva, es un elemento esencial del derecho de acceso a la información pública que requiere de una regulación específica que permita que el Gobierno Nacional adopte medidas conducentes a su protección. Por ende, para esta Sala es prioritario que la AND, como articulador de la política pública digital, con el apoyo del Ministerio Público, como garante del derecho de acceso a la información pública por mandato expreso del artículo 23 de la Ley 1712 de 2014, expidan lineamientos para regular la transparencia algorítmica en los sistemas algorítmicos utilizados por el Estado. Dichos lineamientos deberán propender por la maximización de los estándares de transparencia, confianza y acceso a la información pública y señalar, como mínimo, lo siguiente: (i) las garantías de protección de la transparencia algorítmica en su faceta pasiva; (ii) y las obligaciones del Estado para asegurar que en los próximos desarrollos de herramientas digitales se garantice la faceta activa de este principio, al disponer de forma abierta y periódica de información que permita comprender el diseño y funcionamiento de los algoritmos públicos[176].

---

[176] Un buen ejemplo de instrumento de política pública en la materia se encuentra en la directos sobre sistema de decisión automática (*Directive on Automated Decisión-Making*) expedida por el Gobierno de Canadá. En dicho documento, se establece un principio general de acceso a los componentes digitales algorítmicos del Estado, la publicación de los códigos fuentes de dichas herramientas y los escenarios de auditoría ciudadana a este tipo de aplicaciones. La directriz está disponible en inglés o francés en el siguiente vínculo: https://bit.ly/3uLUZ36.

V. DECISIÓN

En mérito de lo expuesto, la Sala Novena de Revisión de la Corte Constitucional, administrando justicia en nombre del pueblo y por mandato de la Constitución

RESUELVE

PRIMERO.- REVOCAR la sentencia proferida el veinticinco (25) de febrero de dos mil veintiuno (2021) por el Tribunal Administrativo de Cundinamarca, que en segunda instancia confirmó el fallo proferido el dieciocho (18) de enero de dos mil veintiuno (2021) por el Juzgado 64º Administrativo de Oralidad del Distrito Judicial de Bogotá, dentro del trámite de la acción de tutela promovida por el ciudadano Juan Carlos Upegui Mejía en contra de la Agencia Nacional Digital, el Instituto Nacional de Salud y el Ministerio de Salud y Protección Social, quienes fueron vinculados al proceso de tutela de la referencia. En consecuencia, **CONCEDER** el amparo del derecho fundamental al acceso a la información pública del demandante.

SEGUNDO.- ORDENAR al Ministerio de Salud y Protección Social, actual sujeto obligado sobre quien reside la custodia de la información solicitada, que, en un término de quince (15) días hábiles siguientes a la notificación de la presente sentencia, entregue la información solicitada por el actor, esto es, el *código fuente* de la aplicación CoronApp, con todo el historial y control de versiones de dicho código fuente desde su versión original hasta el momento en que estuvo en uso. También deberá informar al accionante si una versión actualizada de ese código fuente se encuentra actualmente en uso en algunas de las aplicaciones de la entidad, y, de ser así, deberá dar igualmente acceso a ese código fuente actualizado y en uso. En caso de evidenciar que parte de ese historial está en custodia de la Agencia Nacional Digital o del Instituto

Nacional de Salud, el Ministerio de Salud y Protección Social deberá requerir a esas entidades para entregar inmediatamente la información ordenada. En éste último evento la Agencia Nacional Digital y el Instituto Nacional de Salud, según sea el caso, deberán entregar la información al Ministerio o directamente al accionante en un término máximo de ocho (8) días siguientes al requerimiento presentado por el Ministerio de Salud y Protección Social.

TERCERO.- ORDENAR al Ministerio de Salud y Protección Social, a la Agencia Nacional Digital y al Instituto Nacional de Salud que, dentro del término otorgado en la orden segunda de la parte resolutiva de esta sentencia, adopte las medidas necesarias para salvaguardar la información personal de los usuarios de la aplicación CoronApp. Si es del caso, para el efecto deberá separar la información correspondiente a los datos personales de los usuarios, almacenarlos en bases de datos y establecer los mecanismos de seguridad pertinentes, tales como credenciales de acceso, contraseñas de seguridad, medios de autenticación y demás medidas que considere pertinentes, con el fin de proteger y custodiar la información personal de los ciudadanos.

CUARTO.- ORDENAR a la Agencia Nacional Digital, en su calidad de entidad articuladora de los proyectos de transformación digital del Estado y los servicios ciudadanos digitales, y a las oficinas designadas por la Procuraduría General de la Nación y a la Defensoría del Pueblo, como entidades que conforman el Ministerio Público en cabeza del cual el artículo 23 de la Ley 1712 de 2014 designó varias competencias para garantizar y monitorear el estado del derecho de acceso a la información pública, que, en un plazo máximo de seis (6) meses contados a partir de la notificación de la presente sentencia, expidan los lineamientos necesarios para que, a partir de la consideraciones de esta decisión, emita lineamientos en relación con la transparencia algorítmica en los sistemas algorítmicos utilizados por el Estado. Dichos lineamientos deberán propender por la maximización de los estándares de transparencia, confianza y acceso a la información pública y señalar, como mínimo, lo siguiente: (i) las garantías de protección de la transparencia algorítmica en su faceta pasiva; (ii) y las obligaciones del Estado para asegurar que en los próximos desarrollos de herramientas digitales se garantice la faceta activa de este principio, al disponer de forma

abierta y periódica de información que permita comprender el diseño y funcionamiento de los algoritmos públicos[177].

QUINTO.- ADVERTIR a la Ministerio de Salud y Protección Social, a la Agencia Nacional Digital y al Instituto Nacional de Salud que, en lo sucesivo, apliquen, como mínimo, los estándares previstos en esta sentencia al momento de estudiar solicitudes de acceso a información pública.

SEXTO.- REMITIR copia de la presente sentencia al Tribunal Administrativo de Cundinamarca, Sección Segunda, Subsección "A" y al Juzgado 64º Administrativo de Oralidad del Distrito Judicial de Bogotá, para que conozcan de la decisión adoptada en el presente proceso.

SÉPTIMO.- ORDENAR al Consejo Superior de la Judicatura que, a través de la Escuela Judicial Rodrigo Lara Bonilla, incluya en sus capacitaciones a los funcionarios judiciales del país contenidos relacionados con la garantía de transparencia algorítmica y su relevancia en el uso y desarrollo de este tipo de herramientas por parte del Estado, haciendo especial énfasis en las implicaciones que ello tiene frente al derecho de acceso a la información pública.

NOVENO.-Por Secretaría General líbrense las comunicaciones previstas en el artículo 36 del Decreto 2591 de 1991.

Notifíquese, comuníquese y cúmplase,

---

[177] Un buen ejemplo de instrumento de política pública en la materia se encuentra en la directos sobre sistema de decisión automática (*Directive on Automated Decisión-Making*) expedida por el Gobierno de Canadá. En dicho documento, se establece un principio general de acceso a los componentes digitales algorítmicos del Estado, la publicación de los códigos fuentes de dichas herramientas y los escenarios de auditoría ciudadana a este tipo de aplicaciones. La directriz está disponible en inglés o francés en el siguiente vínculo: https://bit.ly/3uLUZ36.

NATALIA ÁNGEL CABO

Magistrada

DIANA FAJARDO RIVERA

Magistrada

JORGE ENRIQUE IBÁÑEZ NAJAR

Magistrado

Con aclaración de voto

ANDREA LILIANA ROMERO LOPEZ

Secretaria General

ANEXOS

ACTUACIONES EN SEDE DE REVISIÓN

ANEXO 1: *Amicus curiae* allegados en sede de revisión

Organización Derechos Digitales – América Latina

En oficio del 9 de agosto de 2021[178], la Organización Derechos Digitales – América Latina, manifestó que el razonamiento de la AND y de los tribunales tiene una comprensión limitada de lo que es un código fuente, su funcionamiento, su utilidad y la relación de este con el ejercicio de determinados derechos fundamentales.

Aclara que los programas computacionales o software están escritos en un lenguaje de programación llamado "código fuente", el cual está formado por un conjunto de declaraciones de variables e instrucciones que comúnmente son redactadas por personas con el objetivo de indicarle al programa computacional o software cómo debe funcionar.

La interviniente agrega que el código fuente del software corresponde a los códigos de los programas computacionales y no al programa como tal o a la base de datos que está en poder de quien emplea el software. Así, indica que adicional al "código de fuente" existe el "código objeto", que es el que convierte el código fuente en instrucciones legibles por las máquinas, mediante el proceso de compilación, lo que quiere decir que el código fuente está escrito en un lenguaje que puede ser entendido por el ser humano, mientras que el código objeto está escrito en "lenguaje de máquina". Luego está el "código ejecutable", que reúne elementos, entre ellos, uno o varios códigos objeto, para proveer instrucciones a un sistema informático.

La interviniente concluye que lo que quiere el solicitante es el acceso al código fuente, esto es, el conjunto de archivos con texto en un determinado lenguaje de programación, que representa la fuente original necesaria con las instrucciones de ejecución de un software o programa computacional. La Organización Derechos Digitales agrega que la entrega del código fuente no significa facilitar las llaves de acceso a la base de datos o a un determinado programa computacional, sino solo las instrucciones que ejecutará el programa computacional con el propósito de permitir su examen o modificación.

[178] Cfr. Expediente digital T-8.202.533. Archivo titulado "05AmicusCuriae".

Por tal razón, manifiesta que conocer el código fuente permite analizar, modificar, compartir o copiar el software, mas no necesariamente implica acceder al programa computacional, al sistema informático de otros, a la información almacenada en un sistema informático ajeno, o al dispositivo en cuyo sistema se encuentra instalada una copia distinta del mismo programa computacional. En conclusión, estima la interviniente, el riesgo referido por las accionadas no es claro.

Organización Transparencia por Colombia

En oficio del 6 de agosto de 2021[179], la Organización Transparencia por Colombia indica que el derecho de acceso a la información pública establece una serie de principios orientadores, entre los que resalta el de maximización de la publicidad, la transparencia y la calidad y divulgación proactiva de la información. La interviniente pone de presente que estos principios podrían estar afectados en el caso objeto de revisión, por ausencia del concepto técnico de expertos en la materia que dé claridad, más allá de toda duda, sobre la eventual causación de un daño con la publicación de la información solicitada.

La organización insiste en que la transparencia en la administración pública de la información es fundamental para evitar escenarios de opacidad que promuevan posibles abusos de poder y que puedan ser justificados con la excusa de un presunto riesgo a la salud pública y el interés general. En esa línea, expone que la publicidad del código fuente permite que la ciudadanía ayude a las autoridades públicas a detectar errores de seguridad o a optimizar y complementar las políticas de confrontación a la pandemia. Indica, además, que la participación de la ciudadanía en los asuntos públicos que los afectan permite un adecuado control político de las instituciones y debe ser considerada como un principio general en el que está fundado el Estado colombiano. Además, la ley 1712 de 2014, es clara en establecer que toda persona debe poder acceder a la información pública, comprenderla y

[179] Cfr. Expediente digital T-8.202.533. Archivo titulado "04AmicusCuriae".

analizarla.

Por tal razón, afirma que el derecho de acceso a la información pública y participación ciudadana se está vulnerando por las accionadas, y que deben considerarse las experiencias internacionales, como el caso de España con su aplicación Radar Covid11, cuyo código fue liberado en septiembre de 2020.

Institución Universitaria Politécnico Grancolombiano - Facultad de Ingeniería, Diseño e Innovación

En oficio del 18 de agosto de 2021[180], la Facultad de Ingeniería, Diseño e Innovación de la Institución Universitaria Politécnico Grancolombiano, sostiene que la Agencia Nacional Digital está en la obligación de compartir el código de fuente de la aplicación CoronApp, en especial el de la versión de Android, debido a que es una modificación a un software que se realizó bajo la licencia internacional General Public License, versión 3 (GPL-3.0), el cual está basado en el concepto de "copyleft", que es contrario al concepto de "copyright" (derecho de autor). El fin de este tipo de licencias es la protección del código abierto y la libre distribución, modificación y acceso a los códigos que sean derivados y desarrollados a partir de esta licencia.

En relación con la licencia GPL-3.0 , la GNU GENERAL PUBLIC LICENSE, Versión 3, del 29 de junio de 2007, afirma que "garantiza la libertad para compartir y cambiar las versiones de un programa", indicando la obligación del desarrollador de "respetar las libertades de otros"[181]. La interviniente agrega que esto quiere decir que la licencia GPL no caduca, por lo cual quien recibe un programa que ha sido desarrollado bajo ella está en la obligación de compartir el código fuente con quien lo solicite, independientemente del porcentaje del código original que quede en un

[180] Cfr. Expediente digital T-8.202.533. Archivo titulado "06AmicusCuriae".

[181] Traducciones realizadas por el interviniente y derivadas de la página oficial GNU GENERAL PUBLIC LICENSE, Versión 3, 29 June 2007. Disponible en: https://www.gnu.org/licenses/gpl-3.0.en.html

momento dado. Esto, por cuanto el desarrollador aceptó las condiciones de licencia en un principio y se benefició del trabajo de otros para iniciar su propia versión.

En relación con el código en su versión iOS, aunque no se menciona que usa la licencia GPL-3.0, es probable que las cuestiones de lógica, flujo de información, casos de uso, entre otras consideraciones en el desarrollo del software, se hayan beneficiado del código fuente de la versión de Android.

Por tal razón, la interviniente concluye que, por lo menos en lo relativo a la versión de Android, el desarrollador está en la obligación de entregar el código fuente, en cuanto se trata de código de uso público. En relación con el registro sobre el control de cambios y el historial de versiones del código, indica que ésta es una práctica deseable para: (i) mantener el control sobre las diferentes versiones de la aplicación; (ii) garantizar que, en caso de presentarse fallos, sea posible regresar a versiones funcionales del código; y (iii) para que al incluir nuevas características a la aplicación sea posible hacer pruebas y control de calidad antes de entregar la aplicación compilada al usuario final, motivo por el cual las accionadas deberían llevar este registro.

Adicionalmente, la entidad cuestiona lo manifestado por la AND, en el sentido de indicar que mantendrá el código en reserva hasta que no se cuente con uno definitivo. Al respecto expresa que el "software", por su naturaleza, no puede ser estático y siempre podrá ser sujeto a mejoras, bien sea por actualizaciones en las tecnologías utilizadas, por modificaciones en las condiciones de uso, o por actualizaciones de seguridad, entre otros muchos escenarios. Por tal razón, indica que la afirmación de las entidades accionadas es ambigua, pues no son claras las condiciones que permitirían saber que una versión de la aplicación será "definitiva".

De otro lado, la facultad controvierte que la AND invoque la seguridad de los datos personales de los usuarios, pues la entidad debió desarrollar un

software que permita conocer el código minimizando los riesgos asociados. Para ese propósito existen buenas prácticas como: (i) "el desarrollo por capas", (ii) la "descentralización", (iii) la separación entre la lógica de programa y las credenciales de acceso a las bases de datos donde la información esté almacenada, y (iv) la separación entre la lógica del programa y las direcciones de los servidores en donde se está alojando la información de los usuarios.

Finalmente, la entidad agrega que la documentación usada durante el desarrollo de la aplicación debería ser pública, permitir a las personas hacer una revisión de los componentes y verificar si existe una separación de los datos sensibles recolectados y el código de la aplicación. Esto más aún se justifica en consideración a que se trata de una aplicación desarrollada con recursos públicos.

Centro de Estudios de Derecho, Justicia y Sociedad – Dejusticia

En escrito del 29 de agosto de 2021[182], los investigadores del Centro de Estudios de Derecho, Justicia y Sociedad – Dejusticia-, Maryluz Barragán, Daniel Ospina Celis y Víctor Saavedra, afirman que, en Colombia, toda persona tiene derecho a acceder a cualquier información pública, y por tal razón todo sujeto obligado que decida negar el acceso a esta debe expresar por escrito y de forma motivada las razones para ello, así como adelantar un análisis de legalidad y de proporcionalidad de su decisión.

Los investigadores afirman que el código fuente CoronApp debe ser concebido como un documento o un conjunto de documentos que está bajo posesión, control y custodia de una entidad pública y que, por tanto, está contenido dentro del concepto de "información pública" definido por el artículo 2 de la Ley 1712 de 2014, el cual debe ser compartido en el caso de ser solicitado.

[182] Cfr. Expediente digital T-8.202.533. Archivo titulado "07MemorialDeJusticia.pdf".

Agregan que la AND desconoció el derecho fundamental de acceso a la información pública, ya que: (i) no adelantó un análisis completo sobre las razones por las que el código fuente de CoronApp podía ser exceptuado del acceso efectivo, (ii) tampoco demostró el daño que podría ocasionar la entrega del código fuente y (iii) omitió el análisis sobre la limitación del derecho de acceso a la información pública.

Los investigadores concluyen que las entidades accionadas desconocieron las garantías sustanciales y procedimentales del derecho de acceso a la información pública al aplicar una causal de reserva inexistente en la Ley 1712 de 2014 y omitir demostrar por qué se podría causar un daño presente, probable, específico y significativo al interés abstracto de la protección de datos personales.

Instituto Internacional de Estudios Anticorrupción (IIEA)

En oficio del 31 de agosto de 2021[183], el Instituto Internacional de Estudios Anticorrupción (IIEA) manifiesta que la respuesta de la AND no cumple con las exigencias legales para rechazar el acceso a la información pública, pues la entidad pública que niega el acceso a información que posee, alegando para ello que esta tiene el carácter de reservada, tiene la obligación de demostrar que su decisión no es arbitraria. Ello, indica el interviniente, no ocurrió en esta ocasión.

Para el representante legal del IIEA la decisión del Tribunal Administrativo de Cundinamarca va en contra de las disposiciones de la Ley de Transparencia y Acceso a la Información Pública (Ley 1712 de 20214), ya que admite que la AND omita sus obligaciones en relación con la carga de la prueba y de justificación en relación con la decisión de negar el acceso a la información solicitada.

El interviniente considera que la decisión de la AND de otorgar al código de

[183] Cfr. Expediente digital T-8.202.533. Archivo titulado "08MemorialInstituoAntiCorrupcion".

fuente de la aplicación CoronApp el carácter de reservado (i) no se encuentra sustentada legalmente o constitucionalmente, (ii) carece del "test de daño" que debe realizarse cuando se identifica la presencia de un daño presente, probable, específico y significativo que amerite otorgar reserva a información que, en principio, sería pública, y que (iii) la decisión de tutela no salvaguarda el derecho fundamental de acceso a la información pública. Añade que, en su criterio, la revelación de la información no causaría un daño presente, probable y específico que excede el interés público que representa el acceso a la información.

Para el interviniente impedir que los ciudadanos y usuarios accedan al código fuente de las aplicaciones empleadas por las entidades públicas imposibilita que se pueda hacer un efectivo control de las gestiones y políticas públicas adoptadas por el Estado.

Así, pone de presente que los actuales desarrollos tecnológicos crean la necesidad de renovar y actualizar constantemente los mecanismos de comunicación entre los ciudadanos y el Estado, pues la información que antes se compilaba en hojas, expedientes o archivos ahora se encuentra en aplicaciones o páginas web. Por esa razón, considera que el derecho de acceso a la información pública debe evolucionar a la misma velocidad que lo hacen las tecnologías.

Fundación Karisma

En escrito del 21 de septiembre de 2020[184], la Fundación Karisma remitió una intervención en apoyo de las pretensiones del accionante. La Fundación señala que el derecho de acceso a la información es de carácter instrumental y, a través de él, se ejercen otros derechos, en particular, los relacionados con el escrutinio de la administración pública, la rendición de cuentas por parte del Estado y la gestión de sus representantes y funcionarios.

[184] Cfr. Expediente digital T-8.202.533. Archivo titulado "10AmicusCuriaeFundacionKarisma".

Así, dicha fundación estima que debe imperar el derecho fundamental de acceso a la información siempre y cuando no exista reserva legal expresa[185]. De esta forma, la limitación a este derecho es excepcional y debe estar consagrada de manera previa y expresa en la normativa interna del Estado. También, afirma que, en casos de duda, debe resolverse a favor de la transparencia y el acceso a la información.

Adicionalmente, la fundación agrega que toda negativa al acceso a la información por parte de los funcionarios del Estado debe estar sustentada en el marco legal pertinente y con la carga argumentativa y probatoria correspondiente. De lo contrario, la negativa termina siendo una decisión arbitraria. El interviniente también señala que, en caso de que la autoridad pública haga uso de la Ley 1712 de 2014, es necesario que se supere el test del daño.

En relación con el caso concreto, Karisma encuentra que la negativa al acceso a la información fue arbitraria en su instancia tanto administrativa como judicial, pues a la fecha no hay disposición legal que limite el derecho de acceso a la información en relación con el despliegue y funcionamiento de una aplicación móvil como CoronApp. En ausencia de marco legal vigente, todo análisis en torno a la legitimidad, proporcionalidad y razonabilidad de la negativa carecen, por tanto, de sustento. Igualmente, esta fundación argumenta que la respuesta de la AND no satisface la carga argumentativa y probatoria a la que refiere el derecho interno y que tampoco desarrolla el test del daño.

También, afirma que los jueces de instancia erraron en sus consideraciones, pues parecen confundir el concepto de código fuente con las bases personales asociadas a la aplicación. En ese orden de ideas, Karisma aclara que lo que pide el accionante únicamente refiere al código fuente, cuyo acceso de ninguna manera pone en peligro la intimidad, puesto que se trata de sistemas de información distintos.

[185] Cfr. Sentencia C-491 de 2007.

La Fundación Karisma también hace un recuento de los países que sí publicaron el código fuente de la aplicación móvil para el Covid-19, como lo son Francia, Bélgica, Alemania, España, Estonia, Austria, Holanda, Portugal, Suiza, Canadá, Irlanda, Ecuador, Singapur y Brasil. Se resalta que esa publicación "ha apuntado por reconocer que su acceso por la comunidad experta y demás personas interesadas contribuye al éxito del despliegue y funcionamiento de las aplicaciones móviles para el covid-19, en tanto permite, a partir de la revisión y escrutinio de la ciudadanía, obtener información relevante sobre posibles fallas, vulnerabilidades, entre otros"[186].

Finalmente, la fundación interviniente estima que no hay previsión legal que prohíba la publicación del código fuente bajo consideraciones asociadas al derecho de autor. Por el contrario, debido al uso que se hizo de la Licencia Pública General, la AND tiene la obligación de publicar el código fuente. En efecto, "la GLP le exige [al desarrollador] que ponga a disposición de los usuarios el código fuente modificado, no hacerlo configura una violación a los términos de la misma"[187].

Fundación para la Libertad de Prensa (FLIP)

En oficio del 31 de agosto de 2021[188] la FLIP solicitó que se ampararan los derechos del accionante. Para la Fundación, la AND negó la solicitud del accionante sin cumplir con la carga argumentativa y probatoria exigida por el artículo 28 de la Ley 1712 de 2014 y sin demostrar la existencia de un daño presente, probable, específico y significativo que supere el interés público de suministrar la información.

En esa línea, la FLIP considera que la respuesta de la AND y de los fallos de instancia son contrarios a las garantías constitucionales y al derecho

[186] Ibid. Pg. 8.

[187] Ibid. Pg. 11.

[188] Cfr. Expediente digital T-8.202.533. Archivo titulado "15_09AmicusCuriaeFundacionLibertadPrensa".

internacional al ejercicio de libertad de expresión y el acceso a la información púbica.

Para sustentar su posición, la FLIP insiste en que hay actores que gozan de una protección especial debido a la labor que cumplen en una democracia. En particular, atribuye ese rol al accionante, por el hecho de ser un investigador de una organización defensora de los derechos humanos. Sobre el punto, resalta que el Tribunal Europeo de Derechos Humanos y la Corte IDH han establecido que los defensores de derechos humanos y los periodistas gozan de una protección reforzada en lo relacionado al acceso a la información. Ello, en tanto su labor es fundamental para la democracia y el Estado de Derecho. También sostiene que los defensores de derechos humanos "ejercen un control ciudadano fundamental sobre los funcionarios y las instituciones públicas, al identificar y denunciar violaciones de los derechos humanos, llamar la atención de las autoridades sobre las consecuencias y el impacto de sus acciones y omisiones, y contribuir en la elaboración de políticas públicas que aseguren el cumplimiento de las obligaciones del estado y la efectividad de los derechos" [189]. En ese orden de ideas, la FLIP estima que el acceso a la información forma parte esencial del control democrático.

Por otro lado, la fundación expresa que de acuerdo con el artículo 28 de la Ley 1712 de 2014, cualquier restricción del derecho de acceso a la información pública debe estar motivada e indicar " (i) la disposición legal o constitucional que establece la restricción; (ii) el interés público o particular que persigue dicha restricción; y (iii) la existencia de un daño presente, probable y específico que supera el interés público de la divulgación de la información".[190] Frente a esto, la FLIP encuentra que la negativa de la AND no cumple con los requisitos mencionados, por diferentes razones.

Primero, la entidad solo hizo una mención genérica a la sensibilidad de la

[189] Ibid. Pg. 5.

[190] Ibid. Pg. 7.

información, sin explicar cómo la información implicaría algún tipo de acceso a dicha información (legalidad). Segundo, la AND no esclareció el fin legítimo que busca proteger (finalidad legítima). Tercero, la entidad "se limitó a hablar de una sensibilidad de información que ni siquiera es solicitada"[191] (existencia de daño presente, probable y específico que supera el interés público de la divulgación).

Finalmente, la FLIP agrega que, dado que CoronApp se desarrolló a partir de una licencia de uso público, las entidades accionadas deben "distribuir el software bajo las mismas condiciones de la licencia GPL, lo cual involucra hacer público el código fuente con la finalidad de que pueda ser revisado y utilizado por otros usuarios sin ningún tipo de restricción"[192].

ANEXO 2: Intervenciones allegadas en sede de revisión con ocasión del decreto de pruebas

Procuraduría General de la Nación
En respuesta al auto de pruebas del 5 de octubre de 2021 la Procuraduría expone que el acceso a la información pública tiene tres funciones esenciales: "(i) la garantía de la participación democrática, (ii) posibilitar ejercicio de los derechos constitucionales al permitir conocer las condiciones necesarias para su realización y, (iii) asegurar la transparencia de la gestión pública al constituirse en un mecanismo de control ciudadano de la actividad de la administración"[193]. La Procuraduría estima que la negativa por parte de la AND de entregar el código fuente de CoronApp al accionante no constituye una vulneración de

[191] Ibid. Pg. 9.

[192] Ibid. Pg. 12.

[193] Cfr. Expediente digital T-8.202.533. Archivo titulado. "08RespuestaProcuraduria". Pg. 4.

su derecho al acceso a la información pública, porque tal determinación encuentra sustento en la Ley 1712 de 2014. Lo anterior, en tanto la aplicación en cuestión ha servido como herramienta de suministro de información oficial en temas relacionados con la pandemia ocasionada por el virus del COVID-19 y, a través de ella, el Gobierno Nacional ha recolectado distintos datos de los usuarios como "su nombre, cédula, teléfono, estado de salud, antecedentes médicos, relaciones de parentesco y convivencia, ubicación, así como destinos de viaje, por lo que su operación se encuentra sujeta a las normas de habeas data"[194].

Así, la Procuraduría resalta que, si bien la aplicación puede ser objeto de ataques cibernéticos como cualquier otra aplicación disponible para teléfonos móviles, si se libera ese código se incrementan dichos riesgos, en tanto se "facilita la identificación de las vulnerabilidades del programa y su clonación por medio de técnicas de ingeniería inversa (reversing)"[195].

En conclusión, la Procuraduría estima que la negativa de la AND persigue un fin legítimo como lo es la salvaguarda de la salud pública, toda vez que busca "disminuir la posibilidad de que una herramienta importante para enfrentar el riesgo epidemiológico asociado al coronavirus Covid-19 pueda ser atacada cibernéticamente y, con ello, obstaculizar el desarrollo de las estrategias gubernamentales para controlar la pandemia"[196].

Finalmente, la Procuraduría resalta que la restricción en la divulgación del código fuente de CoronApp no ha impedido el control a la entidad de la gestión sobre la aplicación. Específicamente, expone que se han desarrollado debates políticos al interior del Congreso de la República, se ha llevado a cabo una auditoría externa contratada para tal efecto y, por parte de la ciudadanía, a través del examen de los algoritmos utilizados para su

---

[194] Cfr. Expediente digital T-8.202.533. Archivo titulado. "08RespuestaProcuraduria". Pg. 5.

[195] Ibid. Pg. 7.

[196] Ibid. Pg. 7.

programación, los cuales están disponibles en documentos públicos.

Universidad de la Sabana – Clínica Jurídica de Interés Público y Derechos Humanos

Con ocasión del auto del 5 de octubre de 2021 la Universidad de la Sabana presentó un informe ante la Corte[197]. La universidad explica que la protección del software y de todos sus componentes (incluido el código fuente) hace parte del derecho de autor, especialmente, del área de obras literarias. Sobre el particular, encuentra importante hacer una diferenciación entre la aplicación para iOS y para Android.

Según la universidad, en relación con la aplicación para iOS, la AND se limita a señalar que no utilizó la GPL, y que, en virtud de un memorando de entendimiento suscrito con el Instituto Nacional de Salud (INS), los derechos de autor los ostenta dicha entidad. En ese orden de ideas, considera que lo primero es determinar qué entidad es la titular de los derechos patrimoniales del código fuente para, luego de ello, definir si debe publicarse o no, de conformidad con la naturaleza de la información según la clasificación de la Ley 1712 de 2014.

En relación con la aplicación para Android, la Universidad de la Sabana considera que, en principio, se debe publicar el código fuente, en atención a lo indicado por la AND. En efecto, dicha entidad sostiene que para desarrollar la aplicación en Android utilizó la licencia internacional General Public License (GPL) (versión 3), la cual es de software libre o copyleft. Por ello, la publicación del código fuente, se sigue de la vocación y las obligaciones que emanan del uso de la GPL.

Una vez señalado lo anterior, la universidad precisa que el código fuente es "un archivo o texto simple, escrito en lenguaje de programación con las instrucciones concretas en las que se ejecuta un determinado programa que,

[197] Cfr. Expediente digital T-8.202.533. Archivo titulado. "04RespuestaUniversidadSabana".

dada su sencillez, puede ser leído por cualquier persona que conozca del área"[198]. Dada su naturaleza, y en atención a lo dispuesto por la Ley 1266 de 2008, se puede afirmar que, en principio, se trata de un dato público.

No obstante, la universidad estima que en cada caso se debe verificar que no se trate de una de las excepciones de acceso a la información, según los artículos 18 y 19 de la Ley 1712 de 2014. Ellas se relacionan con posibles afectaciones al derecho a la vida, a la salud o a la seguridad de una persona natural o jurídica.

Para la Universidad en este caso sí se está ante las excepciones de acceso a la información pública contempladas en la ley. En efecto, de publicarse el código fuente "se vería afectado el derecho a la seguridad debido a que, si se logra acceder a los datos de los usuarios, estos podrían llegar a tener un mal tratamiento o ser usados con otros fines y así, su seguridad e incluso su vida podría llegar a verse expuesta ya que al final no se sabe quién podría tener acceso a los datos y cómo los utilizarían".[199]

Adicionalmente, afirma que "si se llegare a publicar el código fuente, se podría atentar directamente a la seguridad nacional (SIC) debido a que se podría tener acceso a la información que los usuarios de CoronApp depositan en la aplicación, como es el caso de la movilidad de los habitantes. Entonces sin distinción sobre si es una persona diplomática o no, se podría tener acceso a sus movimientos y eso atentaría gravemente a la hora de mantener íntegra la seguridad nacional".[200]

Aunado a lo expuesto, señala que la información que recolecta CoronApp tiene la naturaleza de datos semiprivados como el número de teléfono, según las resoluciones 15339 de 2016 y 17607 de 2019 de la Superintendencia de

---

[198] Ibid. Expediente digital T-8.202.533. Archivo titulado. "04RespuestaUniversidadSabana". Pg. 5.

[199] Ibid.

[200] Ibid.

Industria y Comercio (SIC), y los relacionados con el vuelo, la fecha y la aerolínea, en tanto le interesan específicamente al sector salud y al titular, pero no a toda la sociedad.

En conclusión, la universidad insiste en que el juez constitucional, a través de un test de proporcionalidad, debe analizar la tensión entre los derechos a la información pública, la obligación de publicar el código de fuente de la aplicación de Android (por haber usado licencias de uso público) y a la protección de los datos personales, con el fin de determinar si es procedente que la AND publiqué el código fuente.

Eduardo Quijano Aponte

El señor Quijano Aponte dio respuesta al auto de pruebas del 5 de octubre de 2021[201]. En el oficio señala que no encuentra razón alguna para que las entidades accionadas no entreguen al demandante la información requerida.[202]

Fernando Zapata López

En oficio remitido con ocasión del auto de pruebas del 5 de octubre de 2021[203] el señor Zapata López afirma que la protección del software se enmarca en el derecho de autor, de conformidad con lo previsto en el Convenio de Berna. Adicionalmente, señala que la protección del software como obra literaria se extiende a los programas aplicativos, ya sea en forma de código fuente o código objeto.

Por otra parte, expone que el Decreto 1360 de 1989 reglamentó la inscripción del software en el Registro Nacional de Derechos de Autor y que, el artículo 4 de dicha normativa prevé que "el soporte lógico (software)

[201] Cfr. Expediente digital T-8.202.533. Archivo titulado. "02RespuestaEduardoQuijano".

[202] Ibid.

[203] Cfr. Expediente digital T-8.202.533. Archivo titulado. "01RespuestaFernandoZapata".

será considerado como obra inédita, salvo manifestación en contrario hecha por el titular de los derechos de autor".[204]

Finalmente, agrega que el Convenio de Berna establece que las bases de datos hacen parte de las obras derivadas en la categoría de colecciones, las cuales están reguladas en Colombia en la Ley 23 de 1982.

Dirección Nacional de Derecho de Autor (DNDA)

En respuesta al auto de pruebas del 5 de octubre de 2021[205], la DNDA sostiene que los programas de ordenador se protegen bajo el régimen de derechos de autor, lo que otorga a los autores derechos patrimoniales y morales. El código fuente estará protegido cuando cumpla con los requisitos para ser considerado una obra y su protección nace desde su creación, por lo que su registro no es constitutivo sino declarativo. Adicionalmente, resalta que la aplicación CoronApp se encuentra registrada en el libro 11 Tomo 86 Partida 112, como "soporte lógico – software inédito", por lo que estaría protegida por derechos de autor.

La DNA también explica que los derechos morales son intransferibles y siempre pertenecen al creador, pero los derechos patrimoniales pueden ser transferidos mediante un contrato de cesión de derechos de autor, por obra o encargo, o por cesión por ministerio de la Ley. En el primer caso, son requisitos que este conste por escrito y que se haya registrado ante la DNDA para efectos de oponibilidad y publicidad ante terceros. Por su parte, en la obra por encargo ocurre que existe un contrato de prestación de servicios o de obra y se presume que los derechos patrimoniales de las obras que se creen en virtud de estos han sido transferidos al encargante o al empleador. Finalmente, la cesión por ministerio de la ley ocurre cuando el legislador ha determinado la titularidad patrimonial de ciertos tipos de obra radiquen en otras personas, por ejemplo, las obras creadas por funcionarios públicos en

[204] Ibid.

[205] Cfr. Expediente digital T-8.202.533. Archivo titulado. "03RespuestaMinisterioInterior".

cumplimiento de obligaciones constitucionales y legales propias de su cargo serán de titularidad patrimonial de las entidades públicas.

Por otro lado, explica que los titulares de los derechos patrimoniales de autor de un software pueden otorgar licencias de explotación o utilización a terceros, así como hacer fijaciones del programa en su computador personal, una copia de seguridad y una adaptación del programa para su utilización exclusiva.

En relación con el caso concreto, la DNA expresa que las licencias públicas no obligan a publicar el programa modificado ni parte alguna del mismo. La obligación surge en el evento en que se llegue a publicar la versión modificada. Así, la GLP le autoriza a publicar el programa modificado de determinadas maneras y no de otras; pero la decisión de publicarlo o no depende del autor.[206]

Finalmente, la DNA allega un certificado en el que se indica que el Instituto Nacional de Salud es el titular de los derechos patrimoniales de la aplicación CoronApp, a partir del 1 de septiembre de 2021.

Superintendencia de Industria y Comercio (SIC)

Con ocasión del auto del 5 de octubre de 2021[207] la Superintendencia se pronunció dentro del proceso. La SIC señala que su competencia se relaciona con el derecho de propiedad intelectual y no tienen competencias sobre los derechos de autor. Con base en esa precisión, la SIC explica que las patentes representan "una forma de protección en el marco de los derechos de propiedad industrial, la cual una vez es concedida una vez el interesado acredita el cumplimiento de los requisitos establecidos en la decisión 486 de la Comisión de la Comunidad Andina, mediante el trámite

[206] Ibid. Pg. 25.

[207] Cfr. Expediente digital T-8.202.533. Archivo titulado. "06RespuestaSuperintendenciaIndustriaComercio".

contemplado en la referida norma"[208].

En cuanto a la aplicación CoronApp, indica que es un software, en el que la información no es procesada ni transformada por lo que el desarrollo "no se considera como una invención en los términos del artículo 15 de la Decisión 486 de la Comunidad Andina y, por lo tanto, no se podría solicitar la protección de derechos por la vía de la patente de invención" [209].

Adicionalmente, explica que los derechos de propiedad industrial no protegen el software. Por el contrario, la protección que se pudiera otorgar mediante patente recaería sobre los productos o procedimientos que constituyan una "invención implementada por computador". Así, independientemente de si el software es público o no, se deben acreditar los requisitos de patentabilidad (novedad[210], nivel inventivo[211] y aplicación industrial[212]) previstos en el artículo 14 de la Decisión 486 de la Comunidad Andina.

Instituto Nacional de Salud (INS)

Con ocasión del auto del 5 de octubre de 2021[213] el Instituto Nacional de Salud presentó intervención ante la Corte. En primer lugar, el INS afirma que el 1 de octubre de 2021 suscribió el contrato interadministrativo MSPS-485-2021, de cesión total de derechos patrimoniales de autor de la obra CoronApp, en favor del Ministerio de Salud y Protección Social. Ello,

---

[208] Ibid. Pg. 4.

[209] Ibid. Pg. 7.

[210] En este requisito se analiza el estado de la técnica y las características que definen la invención. Así, si existen diferencias entre esas dos, se reconoce que el objeto reclamado es nuevo.

[211] En este ítem se analiza si la invención resulta obvia o se deriva de manera evidente de la información contenida en el estado de la técnica.

[212] Se debe verificar que la invención es susceptible de aplicación industrial, para lo cual se analiza que el producto a procedimiento pueda ser producido o utilizado en cualquier tipo de industria.

[213] Cfr. Expediente digital T-8.202.533. Archivo titulado. "07RespuestaInstitutoNacionalSalud".

pues a la fecha de cesión la aplicación ya había cumplido con la finalidad para la cual había sido creada, pero podría ser de utilidad para el Ministerio de Salud y Protección Social.

Por otro lado, resaltó que "en el evento de ser publicada la versión del código fuente de CoronApp, la aplicación podía resultar expuesta a vulnerabilidades que pondrían en peligro la información recolectada y ello generaría el riesgo de ser utilizada de forma maliciosa o en provecho de terceros no autorizados" [214]. Así, consideró prudente que la publicación del código fuente se hiciera en el momento en que éste se encontrara terminado.

El INS reconoce que los desarrollos de la aplicación son bienes de naturaleza pública. Sin embargo, estima que ellos carecen del carácter de uso público y, por ello, están sujetos a la protección correspondiente de derechos de autor y propiedad intelectual. Además, señala que el código fuente es de interés nacional y por lo tanto "se deben tomar las medidas suficientes para evitar el detrimento de la seguridad nacional, la vulneración de la confidencialidad de la información gubernamental, o que comprometa la razón de su creación al compartirlo"[215]. Para el INS, si se materializan los riesgos, se terminarían por exponer los datos personales de cerca de 13 millones de colombianos, a la vez que se configuraría una inobservancia a los deberes de custodia de los datos sensibles[216].

En relación con la aplicación para iOS, explica que, en virtud de memorando de entendimiento suscrito entre el INS y la AND, ésta fue desarrollada integralmente por la AND y que, por ello, los derechos de autor sobre el software recaen en dichas entidades, hoy en día en el Ministerio de Salud y Protección Social con ocasión de la cesión de derechos.

---

[214] Ibid. Págs. 3 y 4.

[215] Ibid.

[216] Ibid.

Frente a la versión de Android de la aplicación, resalta que efectivamente es una modificación al software de la licencia internacional General Public License, versión 3 (GLP-3.0). Sobre el particular, estima que las mejoras realizadas al código fuente no forman parte de la GLP-3.0 sino que, por el contrario, eran de uso privado del INS[217] (ahora del Ministerio de Salud y Protección Social).

Adicionalmente, señala que otorgar el carácter reservado al código de fuente no supone un incumplimiento por parte del Estado de los términos y condiciones de uso de la licencia pública puesto que se le incorporaron mejoras y se procedió al depósito de la obra ante la Dirección Nacional de Derechos de Autor, la cual quedó protocolizada bajo el Libro 13, Tomo 86, Partida 112, del 1 de septiembre de 2021.

En ese punto, reconoce que el código fuente es sustancialmente distinto de las bases de datos de los usuarios del software. No obstante, al estar íntimamente relacionados uno con el otro, es probable que se use el código fuente para acceder a datos sensibles de los usuarios, los cual afectaría diversos derechos fundamentales. Por ejemplo, es probable que se pueda desarrollar una suplantación de enlaces para el ingreso a la aplicación.

En ese orden de ideas, el INS estima que la no publicación del código fuente garantiza los derechos de autor de CoronApp y salvaguarda los deberes de custodia de datos sensibles.

Por otro lado, y en respuesta a una de las preguntas[218] formuladas por el despacho sustanciador, el INS resalta que toda la información asociada a la

---

[217] Sobre el particular el numeral 6 de los términos y condiciones de CoronApp.

[218] A la luz de las intervenciones realizadas en este trámite, se afirma que incluso de considerarse que existe información objeto de reserva dentro del código de fuente, también hay información que no tendría este carácter. En ese sentido, responda a este Despacho si ¿debe considerarse que la totalidad del código de fuente es reservado o si lo es solo parcialmente? Dado el evento en el que se trate de una reserva parcial, ¿cómo podrían identificarse los elementos objeto de reserva?

aplicación CoronApp se manejó de manera confidencial.

Finalmente, frente a la pregunta en la cual se le solicitaba que expusiera ¿qué debía entenderse como una versión definitiva de la aplicación?, el INS señaló que le corresponde al Ministerio de Salud y Protección Social responder tal cuestión al ser el nuevo titular de los derechos de autor de CoronApp.

Posteriormente, en respuesta al auto del 31 de enero de 2022[219] el INS expresa que, en aras de entender los riesgos técnicos y científicos que podrían materializarse con la publicación de la información solicitada, el código fuente tiene información relacionada con la conexión de desarrollo y, entonces, dar información de este código implica suministrar "información de la estructura de la base de datos, arquitectura, servicios, entre otros" que podría ser usada por los ciberdelicuentes para crear una aplicación similar que pueda confundirse con CoronApp y así la ciudadanía compartiría sus datos personales. En ese sentido, aseguró que esperar a que se tomen controles sobre este tipo de aplicaciones falsas implicaría días en los que pueden tomar la información suministrada por los ciudadanos.

En lo relacionado con la segunda pregunta[220] precisa que no es posible identificar las partes del código fuente que puedan ser publicadas sin necesidad de generar un riesgo, puesto que la entrega parcial del código también puede generar los mismos riesgos de suplantación. Además, refiere que para el funcionamiento del código fuente se requiere que esté completo "so pena de entenderse algo distinto o no representar esencialmente su naturaleza, en la que, si bien se puede dar a conocer una parte de él, no representaría el código fuente integralmente considerado"[221].

---

[219] Cfr. Expediente digital. Archivo titulado "13.3.5.RtaInstitutoNacionalSalud".

[220] ¿Es posible identificar partes del código de fuente que puedan ser publicadas sin necesidad de generar el riesgo aludido?

[221] Cfr. Expediente digital. Archivo titulado "13.3.5.RtaInstitutoNacionalSalud".

La tercera pregunta realizada por el Despacho fue si podrían implementarse las "buenas prácticas de programación" para reducir el riesgo y permitir la publicación de la información solicitada. Al respecto, el INS resalta que el desarrollo de la aplicación tuvo en cuenta estas buenas prácticas. Sin embargo, aduce que no puede publicarse la información, ya que el código "trae parámetros que permitirían acceso a información de carácter reservados y el riesgo de suplantación"[222].

Para dar solución al cuestionamiento plasmado sobre la identificación de la existencia de una versión "definitiva" de la aplicación CoronApp, menciona que esta aplicación fue creada para responder a los requerimientos que surgían con ocasión a la pandemia, y, por tanto, "no podría hablarse de una versión definitiva hasta tanto no termine la pandemia, y la aplicación deje de ajustarse conforme a los requerimientos de la realidad epidémica de cada momento"[223].

Finalmente, explica que la expresión de "ya se cumplió" con la "finalidad" quiere decir que se había cumplido con la fase de mitigación para octubre de 2021, y posteriormente, con ocasión a la cesión celebrada con el Ministerio de Salud, es éste quien entra a administrar la aplicación y a determinar sus funcionalidades y alcances para que se adapte al desarrollo propio de la pandemia.

Juan Carlos Upegui Mejía

Con ocasión del auto de pruebas del 5 de octubre de 2021 el accionante envió un oficio a la Corte[224]. Para el señor Upegui Mejía este caso resulta de especial importancia como un precedente que puede ser útil para el país y, en general, para la región. Como primera medida, destaca que el código

[222] Ibid.

[223] Ibid.

[224] Cfr. Expediente digital T-8.202.533. Archivo titulado. "05RespuestaJuanCarlosUpegui".

fuente de la aplicación debe ser considerado como información pública y que, por regla general, solo puede negarse el acceso a esta si las entidades públicas cumplen con ciertas condiciones y exigencias argumentativas y demostrativas.

En ese sentido, considera que indistintamente del fondo de la discusión, su derecho al acceso a la información pública fue vulnerado, pues las accionadas le negaron el suministro de la documentación objeto de litis, sin desplegar la carga argumentativa requerida para el efecto[225]. A su juicio, las entidades accionadas, a pesar de los numerosos pronunciamientos que han realizado dentro del presente trámite, no han podido probar la existencia del supuesto daño, el cual, de llegarse a materializar, no tendría que ver con la publicación del código de fuente, sino con el desarrollo de "malas prácticas de programación"[226] que restan seguridad a la aplicación y a las bases de datos que maneja.

El accionante afirma que las accionadas han vulnerado sus derechos fundamentales, pues si consideraban que podía haber distintos tipos de información, una reservada y otra no, les correspondía realizar distintas versiones que permitan el acceso a la información que no tiene carácter reservado. En ese sentido, considera que las entidades accionadas, para evitar riesgos, hubieran podido ocultar la información con capacidad de crear vulnerabilidades, sin que, por ello, sea necesario impedir el acceso a la totalidad del código.

De otro lado, destaca que es falaz el argumento de las accionadas en relación con que la eventual publicación del código de fuente afectaría los derechos de autor del titular de la obra, pues, en su criterio, "la revelación de

---

[225] En concreto, indica que le correspondía a las accionadas demostrar: (i) que la entrega de la información solicitada afecta intereses previstos en los artículos 18 y 19 de la Ley 1712 de 2014; (ii) que existe un fundamento legal o constitucional que fundamenta la negativa; y (iii) que conceder el acceso a la información podría causar un daño "presente, probable, específico y significativo" que excede el interés público que representa el acceso a la información pública.

[226] Ibid. Pg. 5.

la información pública per se no tiene incidencia alguna, no puede tenerla, sobre los derechos de autor" [227]. Para el demandante, "la afectación de los derechos de autor, debido a su contenido patrimonial, solo se concreta si se produce una explotación económica de la información protegida con dichos derechos o, debido a su contenido moral, se busca suplantar la aplicación o la autoría" [228]. Por ello, considera que la simple divulgación de la información protegida no es incompatible con el régimen jurídico de los derechos de autor.

Sobre este tema, el demandante también subraya que: (i) no puede existir ninguna afectación a los derechos patrimoniales que se deriven del régimen de derechos de autor, pues la aplicación CoronApp es totalmente gratuita; y (ii) el presunto riesgo de suplantación al que se hace referencia es "prácticamente imposible" pues, por la naturaleza de la aplicación, las plataformas de Apple y Google cuentan con restricciones para la publicación y comercialización de este tipo de apps.

Finalmente, el demandante sostiene que, de existir vulnerabilidades en la programación, que podrían comprometer la información de los colombianos, la publicación del código fuente se hace aún más necesaria o, en otros términos, sería más beneficiosa que perjudicial. Esto se debe a que permitir que el público revise el código podría ayudar a identificar y solucionar dichas vulnerabilidades, mejorando la seguridad de los datos.

Agencia Nacional Digital (AND)

La Agencia se pronunció sobre las pruebas recaudadas mediante el auto del 5 de octubre de 2021[229]. En primer lugar, afirmó que la titularidad de los derechos patrimoniales no reposa en la AND y que, con el Instituto Nacional de Salud (INS) se determinó que "en el evento de ser publicada la versión

[227] Ibid. Pg. 7.

[228] Ibid.

[229] Cfr. Expediente digital T-8.202.533. Archivo titulado. "01RespuestaAgenciaNacioanlDigital-AND".

del código fuente de CoronApp, la aplicación podría resultar expuesta a vulnerabilidades que pondrían en peligro la información recolectada y ello generaría el riesgo de ser utilizada de forma maliciosa o en provecho de terceros no autorizados" [230]. En ese orden de ideas, la AND señala que la publicación del código fuente podría hacerse cuando éste se encuentre terminado.

En segundo lugar, la AND precisa que los desarrollos de la aplicación no son de carácter de uso público y que por ello están cubiertas por la protección propia de los "derechos de autor de propiedad intelectual (SIC)", además de la protección a los derechos de los titulares de la información registrada en la aplicación, a quienes se les debe garantizar privacidad y seguridad. En ese sentido, precisó que el código fuente de CoronApp es de interés nacional y, por lo tanto, "se deben tomar las medidas suficientes para evitar el detrimento de la seguridad nacional, la vulneración de la confidencialidad de la información gubernamental, o que se comprometa la razón de su creación al compartirlo. El impacto generado, producto de la materialización de dichos riesgos, podría causar que se expongan datos personales de cerca de 13 millones de colombianos afectando derechos fundamentales en todo el territorio nacional, a la vez que configuraría una inobservancia a los deberes de custodia de los datos sensibles".[231]

En tercer lugar, la AND reitera que la publicación del código fuente generaría un riesgo de suplantación tecnológica.

La AND aclaró que el 1º de octubre de 2021 el INS, a través de contrato interadministrativo de cesión total de derechos patrimoniales de autor, cedió la obra CoronApp a favor del Ministerio de Salud y Protección Social.[232]

---

[230] Ibid. Pg. 3.

[231] Ibid. Pg. 4.

[232] Contrato MSPS-485-2021. Objeto: "El cedente (Instituto Nacional de Salud INS) transfiere de manera total, exclusiva, gratuita y sin limitación alguna al cesionario (Ministerio de Salud y Protección Social – MSPS) los derechos patrimoniales de autor que ostenta respecto de la obra denominada CoronApp Colombia"". Este contrato puede consultarse en SECOP II.

Finalmente, sostiene que concuerdan con la Procuraduría General de la Nación en que la negativa de entregar el código fuente al accionante persiguió un fin legítimo, el cual es la salvaguarda de la salud pública y la protección de los datos personales de los usuarios de la aplicación[233].

La AND también dio respuesta al auto del 31 de enero de 2022[234]. Frente a los razonamientos técnicos o científicos sobre los riesgos que podrían materializarse con la publicación de la información, refiere que entregar el código fuente implica suministrar información de la estructura de la base de datos y la forma de conexión a la misma, lo cual "representa un riesgo extremo al revelar la estructura lógica del funcionamiento y por lo tanto dar a conocer insumos a los ciberdelincuentes para diseñar vectores de ataque que puedan materializarse en incidentes de alto impacto".

Adicionalmente, indica que no es posible publicar partes del código fuente sin generar riesgos, pues de hacerse implicaría la realización de un nuevo código, ya que "el código fuente para que funcione requiere de todo lo que lo contiene y de cada una de las líneas que hace parte de él so pena de entenderse algo distinto o no representar esencia.

Posteriormente, la AND se pronunció acerca de las pruebas recaudadas mediante el auto del 31 de enero de 2022[235]. En este documento la AND señala que los "desarrollos de la aplicación son bienes naturaleza pública", pero no tienen el "carácter de uso público", y que del "desarrollo de la aplicación CoronApp se derivan derechos de autor y derechos de los

---

[233] Como documentos anexos, allegó los siguientes: (i) texto del "clausulado anexo al contrato interadministrativo de cesión de derechos patrimoniales de Autor No. 485 de 2021, suscrito entre el Ministerio de Salud y Protección Social e Instituto Nacional de Salud (INS)"; (ii) texto del "clausulado anexo al contrato interadministrativo No. 720 de 2021, suscrito entre el Ministerio de Salud y Protección Social y Corporación Agencia Nacional Digital (AND)" y (iii) términos y condiciones de uso de la aplicación CoronApp.

[234] Cfr. Expediente digital. Archivo titulado "13.3.6RtaAgencionaNacionalDigital.pdf".

[235] Cfr. Expediente digital. Archivo titulado "13.5.2RtaTrasladoAgenciaNacionalDigital.pdf".

titulares de la información registrada en la aplicación". A unos y otros se les debe garantizar la privacidad y la seguridad requerida. Por lo anterior, la AND argumentó que el juez constitucional debe hacer una evolución desde la óptica de los derechos relacionados con la propiedad intelectual. Mencionó, además, que el trámite de la aplicación está protegido por el artículo 61 constitucional.

Aunado a lo anterior, manifestó que "nos encontramos frente a la situación de excepcionalidad reserva legal contemplada dentro de las excepciones de acceso a la información de que tratan los artículos 18 y 19 de la Ley 1712 de 2014". De otra parte, señaló que no se puede escindir el acceso a la información de cada uno de los usuarios del código de la aplicación, pues "están estrictamente ligados en virtud del desarrollo realizado" [236].

Finalmente, en escrito del 22 de junio de 2022[237], la AND se pronunció respecto de las respuestas otorgadas por los intervinientes al auto de pruebas del 13 de mayo de 2022. En primer lugar, la AND reitera que la publicación del código fuente podría facilitar la simulación de la aplicación para el robo de datos personales, así como el desarrollo de sitios ficticios de descarga.

En segundo lugar, la AND explica cuándo se considera que un código fuente ha llegado a su iteración final. Expone que esa es una decisión del propietario del código, quien define cuándo se logra el objetivo final de este y decide no darle más soporte. Sin embargo, mientras los propietarios de la aplicación CoronAPP, Ministerio de Salud e Instituto Nacional de Salud, no decidan dejar de darle soporte a la aplicación, sí es posible actualizar el código y mejorar sus parches de seguridad.

---

[236] Cfr. Expediente digital T-8.202.533. Archivo titulado. "AND-EXT-00159 Pronuncuamiento sobre las Pruebas Expediente No. T-8.202.533 Acción de Tutela Juan Carlos Upegui Ofi. No. OPTC-061-2022 - Corte Constitucional"

[237] Cfr. Expediente digital T-8.202.533. Archivo titulado. "AND-EXT-00159 Pronuncuamiento sobre las Pruebas Expediente No. T-8.202.533 Acción de Tutela Juan Carlos Upegui Ofi. No. OPTC-061-2022 - Corte Constitucional"

En tercer lugar, la AND indica qué medidas de protección se podían tomar en caso de que se publique el código fuente de CoronAPP. Primero, señala que, en la actualidad, CoronAPP no es una aplicación de código abierto y, en caso de que se haga público es necesario que se tomen medidas tales como evitar liberar las partes relacionadas con el almacenamiento de información. Del mismo modo, la AND recomienda que en ese caso se siga la Política de Datos Abiertos del Ministerio de Tecnologías de la Información.

En cuarto lugar, sobre la pregunta por buenas prácticas cuando el Estado revela el código fuente de alguna de sus aplicaciones, la AND dice que en Colombia no existe una lista de ellas. Sin embargo, refirió que la OCDE cuenta con 10 principios de buenas prácticas para estos casos.

En quinto lugar, la AND señala que en caso de que se libere el código fuente de la aplicación, una de las medidas necesarias es la anonimización y seudoanonimización. Para esto es necesario utilizar las herramientas técnicas que describe la Ley 1582 de 2012.

En sexto lugar, la AND explica los riesgos para la propiedad intelectual en caso de que se hiciera público el código fuente. Así, expone que publicar el lenguaje de programación no representa riesgos de propiedad intelectual, pero publicar el código fuente sí.

La AND expone que en caso de publicar el código fuente es necesario seguir las recomendaciones de Colombia Compra Eficiente en su Guía de buenas prácticas en la adquisición de Software y servicios asociados. No obstante, la AND resalta que una vez el código fuente se hace público el autor pierde el control sobre la obra.

Ministerio de Salud y Protección Social
El Ministerio de Salud y Protección Social dio respuesta al auto del 31 de enero de 2022.[238] En su escrito, el Ministerio desarrolla el marco jurídico de protección del código fuente como obra sujeta a los derechos patrimoniales de autor y la normativa interna del Instituto Nacional de Salud sobre propiedad intelectual. Al respecto, destaca que la aplicación móvil Coronapp fue registrada ante la Dirección Nacional de Derechos de Autor y que, en consecuencia, es sujeta de derechos de propiedad intelectual. A partir de la cesión de los derechos de autor hecha por parte del INS al Ministerio, es este último quien tiene los derechos patrimoniales sobre la obra. El Ministerio también explica que, de acuerdo con la normativa interna del INS, la información no divulgada que posea legítimamente el INS y que tenga un valor técnico, científico, estratégico o legal que sea susceptible de transmitirse a un tercero es considerada como secreto empresarial. En suma, la entidad argumenta que el Ministerio de Salud, como cesionario de los derechos de autor sobre la aplicación CoronApp, puede oponerse a la entrega del código fuente al accionante, pues dicha obra no puede ser considerada pública. Luego, el Ministerio explica el manejo que le ha dado a la aplicación Coronapp desde la cesión y las nuevas funcionalidades que se le añadieron, que llevaron a que la aplicación evolucionara a una nueva, denominada Minsalud Digital, que no puede considerarse un producto terminado ni nuevo. Finalmente, el Ministerio explica que no ha publicado ni pretende publicar el código fuente del aplicativo Minsalud Digital, pues se trata de un activo critico en cabeza de la entidad que podría afectar la confidencialidad e integridad del Ministerio. En concreto, indicó que existe un alto riesgo de suplantación de la aplicación. Posteriormente, el Ministerio se pronunció sobre el traslado de las pruebas

[238] 13.3.3RtaMinSalud.pdf

recaudadas en virtud del auto del 31 de enero de 2022[239] y agrega que exponer el código fuente a internet puede causar suplantación de la aplicación y "permitir la captura de datos de los ciudadanos colombianos entre ellos datos sensibles"[240]. Por estas razones, reitera lo expuesto en la intervención allegada y solicita no acceder a las pretensiones del demandante.
Defensoría del Pueblo
Con ocasión del auto del 31 de enero de 2022[241] la Defensoría del Pueblo intervino en el proceso. La delegada de la Defensoría considera que la AND vulneró el derecho de petición del actor, pues la respuesta esgrimida, en relación con el riesgo de dar información sobre el código fuente de la aplicación CoronApp, no tiene sustento legal ni constitucional. Según la Defensoría, la entidad no probó el eventual riesgo de información sensible de los usuarios de la aplicación. Por tanto, infiere que la acción de tutela es procedente, siempre que no afecte los datos sensibles de los usuarios.
Universidad Nacional de Colombia
En respuesta al auto del 31 de enero de 2022 la Universidad expone que la aplicación CoronApp recepciona datos que pueden considerarse de carácter privado, público y sensible y, por ende, el Estado es el encargado del tratamiento de estos datos. Asimismo, señala que esta aplicación fue "desarrollada bajo una licencia de software libre, GNU General Public License, versión 3 (GPL-3.0)", cuya principal característica es el acceso al código fuente que permite al usuario hacer uso de éste y modificarlo; además "trae consigo una obligación de licenciar el nuevo programa de ordenador bajo las mismas condiciones otorgadas en la licencia inicial o unas condiciones similares"[242].

[239] Cfr. Expediente digital. Archivo titulado "MINSALUD_RTA_PRUEBAS1202242300626192_00003".

[240] Ibid.

[241] Cfr. Expediente digital. Archivo titulado "13.3.1RtaDefensoria".

[242] Ibid.

Asevera que al publicar el código fuente pueden exponerse vulnerabilidades asociadas a este; así, indica investigaciones realizadas en 2020 que "evidencian que el 84 % de los repositorios de código fuente auditados contenían al menos una vulnerabilidad, de las cuales el 60 % eran de alto riesgo y que personas con intereses diferentes a los de mejorar el código aprovechan para explotar la vulnerabilidad, por lo que siempre que se exponga el código fuente conlleva riesgos de seguridad"[243]. De manera que la publicación el código fuente de la aplicación CoronApp implicaría ciertos riesgos de seguridad, en la medida que revelaría el software sobre el que se construyó la aplicación, lo que facilitaría un ataque sistemático.

Aunado a lo anterior, indica que con la publicación del código fuente se pone en riesgo la seguridad por ataques al software y, con ello, a la base de datos personales sensibles, privados e información pública reservada. Sin embargo, concluye que el requerimiento de la información solicitada por el actor puede ser resuelta "con la entrega de la descripción del programa o material auxiliar, en los términos de los numerales 2 y 3 del artículo 2.6.1.3.3 del Decreto Único Reglamentario del Sector Administrativo del Interior Decreto 1066 de 2015, sin que sea necesaria la entrega del Código fuente y sus respectivas modificaciones (Programa de computador)"[244].

INNpulsa

INNpulsa Colombia indicó que el código fuente de una aplicación pública como CoronApp no contiene información personal. Sin embargo, compartir el código fuente de un software sí puede permitir que se conozca la arquitectura técnica y la construcción del sistema operativo, lo cual podría generar fallas de seguridad del sistema y podría enfrentar contingencias de acceso o uso indebido de la información que está en la aplicación. Para INNpulsa hacer público el lenguaje de programación de la aplicación no solo permite que se obtenga información de cómo opera desde el punto de

[243] Ibid.

[244] Ibid.

vista funcional y técnico, sino que puede generar casos de “Phishing”, “Pharming”, “Smishing”, “Whailing” y “Link Manipulation”.

Adicionalmente, explica que el código fuente siempre puede ser editable y por lo tanto susceptible de cambios. Igualmente, aclara que la iteración final significa que se está en una parte del proceso que permite llegar a un producto utilizable, pero no es sinónimo de imposibilidad de edición del código fuente.

En relación con las medidas de seguridad que puede implementar el Estado para garantizar la seguridad informática y la protección de los datos personales en caso de hacerse público el código fuente de CoronApp, INNpulsa sostiene que deberían implementarse medidas de bloqueo en materia de datos sensibles, por lo que podría considerarse anonimizarlos, con lo cual se tendría acceso a los datos en general, sin incluir las condiciones de salud de cada ciudadano. Adicionalmente, explica que se deberían aplicar medidas tecnológicas efectivas.

En cuanto a las buenas prácticas, explica que tradicionalmente han existido medidas que permiten asegurar el código de fuente, como, por ejemplo, (i) el principio del mínimo privilegio que permite que los permisos que se le den a un usuario sean mínimos y estén focalizados para la ejecución de ciertas funciones; (ii) limitar el acceso del administrador y (iii) realizar revisiones periódicas del código fuente.

Por otra parte, sostiene que el literal d) del artículo 17 de la Ley 1581 de 2012 señala como uno de los deberes de quienes son responsables del tratamiento de datos el de conservar la información bajo condiciones de seguridad, y que el principio de seguridad debe orientar el tratamiento de datos. En ese entendido, señala que no debería permitirse una situación que pueda generar riesgos sobre los datos de una aplicación que contiene datos sensibles y que un ejemplo del manejo, almacenamiento y custodia de la información está contenido en la Política de Datos Personales de la

Superintendencia de Industria y Comercio que señala que el almacenamiento de la información digital y física se debe realizar en medios que cuenten con adecuados controles para la protección de datos.

Finalmente, sugiere que se revise la política y los lineamientos para anonimizar los datos del Ministerio de Salud y la rigurosidad de la aplicación de los mismos para que no haya fugas de datos. Además, indica que se debe garantizar una medida técnica o tecnológica que aísle de manera efectiva la base de datos o el soporte donde están almacenados los datos para separarlos completamente del código fuente de la aplicación.

En relación con la sexta pregunta, sobre el riesgo que supondría para la propiedad intelectual y los derechos de autor el hacer público el lenguaje de programación del código fuente de una aplicación desarrollada por el Estado, INNpulsa explica que el que una aplicación sea desarrollada por una entidad pública y que la herramienta sea de uso público, aunque se trate de software abierto, no significa que el sistema operativo, como obra, sea de dominio público. En ese sentido, refiere al literal l) del artículo 4 de la Decisión 351 de la Comisión de la Comunidad Andina, que indica que los programas de ordenador son obras que pueden ser protegidas por el derecho de autor. Así mismo, señala que para el caso concreto debería revisarse la licencia GPL y sus términos y condiciones respecto del uso de ese sistema operativo y del acceso que terceros puedan tener respecto al código fuente.

Por otra parte, INNpulsa explica que los derechos patrimoniales permiten controlar la explotación económica de la obra y que son oponibles a terceros, de forma tal que cualquier acto que impida o limite su explotación debe ser considerado como un riesgo para la propiedad intelectual. Cuando las obras son realizadas por empleados públicos o por contratistas del Estado, la Ley 23 de 1982 dispone que opera la cesión por ministerio de la ley, lo cual no equivale a que la obra entre al dominio público. En estos casos también debe tenerse en cuenta que los derechos de autor incluyen los derechos morales de la persona natural que realizó la obra, por lo que entregar el código fuente de una aplicación limitaría el ejercicio de los

derechos patrimoniales y morales de autor.

Finalmente, en relación con la última pregunta, acerca de las precauciones que se deben tomar para proteger la propiedad intelectual y los derechos de autor en caso de que un código de fuente se llegara a hacer público, sostiene que, en ese evento, a su juicio, el titular de los derechos patrimoniales de autor perdería el control de su obra, por lo que no es aconsejable que se permita el acceso al código fuente, a menos que se cuente con una autorización, licencia o cesión de su titular. En este sentido, sugiere que podría dársele al código fuente un tratamiento de secreto empresarial, para lo cual el poseedor de la información podrá adoptar todos los mecanismos que considere necesarios para lograr su confidencialidad. Lo anterior implica que el Estado no entregue el código fuente a ningún tercero, con fundamento en la excepción contenida en el literal c) del artículo 18 de la Ley 1712 de 2014, que versa sobre la negativa de acceso a la información cuando se trata de secretos comerciales, industriales y profesionales.

Para terminar su exposición explica que la protección del software tiene un sustento constitucional en el artículo 61 y que por ello el Estado debe impedir que se afecte el normal ejercicio de la propiedad intelectual.

Departamento Nacional de Planeación

El Departamento Nacional de Planeación dio respuesta a los interrogantes planteados por el despacho en el auto del 13 de mayo de 2022. En primer lugar, sobre los riesgos en términos de “phishing”, “pharming”, “smishing” y otros, que puede representar la publicación del código fuente, la entidad ahonda en la definición de cada uno de ellos y explica que ese tipo de ataques tiene en común la ingeniería social, por lo que no alteran la tecnología como tal, sino que se aprovechan de los errores y las conductas humanas a través de engaños. Por ello, la entidad concluye que compartir el código fuente realmente no expone a los usuarios a ese tipo de ataques pues el atacante utilizará otro tipo de recursos diferentes al código, como copiar la imagen institucional en un mensaje o falsear un sitio web para engañar a

los usuarios.

En segundo lugar, el Departamento explica que si bien se puede entender que el código fuente llega a su iteración final cuando cumple con el propósito para el que fue creado, ello no implica que no se le sigan haciendo cambios y modificaciones.

En tercer lugar, frente a las medidas de seguridad para proteger los datos personales de los usuarios de la aplicación, explica que hay esquemas de seguridad específicos que deben seguirse cuando se construye cualquier código fuente. Así, existe el Modelo de Seguridad y Privacidad de la Información del MinTic que busca que las entidades del Estado implementen las mejores prácticas de seguridad para proteger los datos de los ciudadanos.

Adicionalmente, indicó que si bien no existe un consenso en la literatura sobre las mejores prácticas frente a la publicidad de códigos fuente, hay recomendaciones generales que puede adoptar el sector público para implementar el software abierto en proyectos y aplicaciones. Por ejemplo, los "Principios de buenas prácticas para la ética de datos en el sector público" de la OCDE en los que se propone que los servidores públicos identifiquen los posibles riesgos en la utilización de datos y tomen las medidas apropiadas para mitigarlos, y se enfatiza en la importancia de que el código fuente sea abierto al público para fomentar la transparencia, especialmente en proyectos que traten datos personales o sensibles de la comunidad. Por ello, como medida de protección de los datos, el Departamento propone la anonimización de los mismos antes de la publicación del código fuente.

Finalmente, la entidad explica que los códigos fuente son protegidos por el derecho de autor y que la publicación de estos puede poner en riesgo dichos derechos. Sin embargo, aclara que la apertura del software puede tener diversos grados de tal forma que no se pongan en riesgo esos derechos. La

entidad señala que si se trata de un software propietario (es decir que no tiene licencia abierta), la publicación masiva puede acarrear riesgos de que se realicen copias no autorizadas por lo que sería prudente controlar el público que accede al mismo.

Universidad Externado de Colombia

La universidad Externado de Colombia respondió a los interrogantes del auto del 13 de mayo de 2022. En primer lugar, la universidad aclara que si bien es posible que usuarios malintencionados utilicen el código fuente para engañar a usuarios, la posibilidad de que ello pase es mínima pues las tiendas de aplicaciones tienen medidas de seguridad para evitar que ello ocurra.

En segundo lugar, la universidad indica que la iteración final de un código fuente es difícil de determinar, pues pueden surgir nuevas necesidades y la aplicación puede requerir mejoras. Sin embargo, si se está en un contexto de contratación estatal, se puede entender que el código es entregable una vez cumple con el objeto contractual, aunque puede ser objeto de futuras actualizaciones.

En tercer lugar, frente a las medidas de seguridad para garantizar la protección de los datos personales de los usuarios, la universidad menciona las regulaciones que existen en el país frente al tratamiento de esos datos. En particular, destaca que el Decreto 1078 de 2015 obliga a los prestadores de servicios ciudadanos digitales a que realicen una evaluación de impacto de las operaciones de los servicios y esa evaluación de impacto, en su parecer, puede ser una buena medida previa a la publicación del código fuente. La universidad también destaca que la protección de los datos se puede garantizar aplicando medidas de seguridad desde el diseño de las aplicaciones. Igualmente, menciona como ejemplo el caso de Australia en donde se publicó el código fuente tras tomar algunas medidas de seguridad como una revisión previa por agencia de seguridad, y la eliminación de algunas partes del código fuente relacionadas con el almacenamiento de la

información.

En cuarto lugar, la universidad hace un listado de las que considera buenas prácticas para reducir los riesgos asociados a la publicación del código fuente, entre las que se destacan el encriptado y el manejo de llaves y claves de acceso.

Finalmente, para proteger la propiedad intelectual y los derechos de autor, la universidad sugiere que en los contratos de licencia de software que celebre el estado se consagre expresamente que la entidad podrá publicar el código fuente respetando los derechos morales. También considera importante que se haga el registro del software ante la Dirección Nacional de Derechos de Autor y que, antes de publicar el código se publiquen unos términos y condiciones que deben respetar los ciudadanos que accedan al código.

Agencia Analítica de Datos - Agata

La Agencia Analítica de Datos -Agata- respondió al requerimiento hecho por la Corte en el auto del 13 de mayo de 2022. En primer lugar, sobre los riesgos asociados a la publicación del código fuente, la agencia señala que estos se materializan si la aplicación no ha sido desarrollada bajo un proceso de desarrollo de software seguro. En segundo lugar, indica que el código fuente nunca tendrá un estado final absoluto, pues requiere de constantes actualizaciones.

En tercer lugar, sobre la protección de los datos personales, manifiesta que si existen medidas que pueden garantizar su seguridad. Así, específica que todas las entidades públicas deberían implementar técnicas de desarrollo seguro y cumplir con el Modelo de Seguridad y Privacidad de la Información. También se pueden tener en cuenta otras prácticas como la de codificación segura que implica adoptar medidas como el uso de controles de acceso, practicas criptográficas y de gestión de archivos. Sin embargo, la

agencia también explica que específicamente para la protección de datos personales, el control más ampliamente utilizado es la anonimización y la pseudoanonimización y hace un desarrollo de esos conceptos.

En cuarto lugar, Agata explica que los códigos fuente están protegidos por derechos de autor y que pueden hacer parte del patrimonio del Estado, dándole la facultad para decidir si los publica o no. Aclara también que, si el Estado adquiere una licencia sobre un software, deberá respetar los términos y condiciones establecidos en esa licencia para su publicación. En todo caso, para mitigar los riesgos a la propiedad intelectual y derechos de autor, la agencia indica que el Estado debe publicar disclaimers advirtiendo sobre la titularidad del código y los usos y prohibiciones aplicables a terceros que pueden llegar a acceder al mismo.