

Sentencia T-058/15

DERECHO AL HABEAS DATA-Justificación histórica del poder informático

DERECHO AL HABEAS DATA-Alcance en el ámbito nacional e internacional

DERECHO AL HABEAS DATA-Derecho a la autodeterminación informativa o informática

CLASES DE INFORMACION-Pública, semiprivada, privada y reservada

PRINCIPIOS QUE DEBE SEGUIR EL ADMINISTRADOR DE BASES DE DATOS-Finalidad, necesidad, utilidad y circulación restringida

ACCESO DE DATOS PERSONALES COMO EXPRESION DEL PRINCIPIO DE ACCESO Y CIRCULACION RESTRINGIDA-Refuerza el carácter individual del dato y evita que la información contenida en una base de datos se utilice para finalidades distintas a aquella que motiva su existencia

CERTIFICADO DE ANTECEDENTES JUDICIALES-Evolución normativa

CERTIFICADO DE ANTECEDENTES JUDICIALES-Naturaleza y funciones

Considerando la importancia que tienen las bases de datos relacionadas con antecedentes judiciales en el marco del Estado Constitucional y que su existencia obedece a legítimos fines de la misma estirpe, esta Corte ha señalado que su registro no puede ser considerado como una sanción. En efecto, si bien los antecedentes penales son el producto de la imposición de un castigo, no son la pena en sí misma ni adquieren autonomía punitiva. En todo caso, lo anterior no quiere decir que la información sobre antecedentes judiciales no pueda ser suprimida de forma relativa de acuerdo con la conciliación de varios elementos normativos que concurren en el caso de la administración de información personal en esta materia.

CERTIFICADO DE ANTECEDENTES JUDICIALES Y HABEAS DATA-Efectos de la sentencia SU458/12

TRANSFERENCIA INTERNACIONAL DE DATOS PERSONALES-Exigencia de estándares de protección

Se entiende que la exigencia de estándares de protección equivalentes para la transferencia internacional de datos, es una pauta que por su vocación principalística no solamente puede aplicarse en forma sectorial o a un tipo específico de bases de datos pese a que la legislación colombiana en materia de hábeas data ostente dicho carácter, sino que es de aplicación común y en ese sentido, tal principio, como sus excepciones constituyen herramientas para la solución de casos en los que se hallen involucradas bases de datos relacionadas con antecedentes judiciales. En efecto, encuentra la Corte que dicha excepción al principio de transferencia de datos referida en el párrafo anterior, constituye por sí misma la expresión de otro principio, el de libertad. En ese sentido, se entiende que dicha excepción, relacionada con la voluntad del titular para dar a conocer información personal a un tercero por él indicado, en este caso su registro de antecedentes judiciales a otro Estado, es plenamente admisible de conformidad con el entendimiento jurisprudencial sobre la aplicación principalística de la Ley 1581 de 2012, particularmente en lo que hace al principio de libertad en la administración de datos personales.

SOLICITUD DE CERTIFICADO DE ANTECEDENTES JUDICIALES POR GOBIERNO

EXTRANJERO CON FINES MIGRATORIOS-Tiene un propósito legítimo en el marco del bloque de constitucionalidad

La Sala encuentra que, en primer lugar, la solicitud del certificado de antecedentes judiciales por un Gobierno extranjero para la autorización de migrar hacia su territorio obedece a un propósito legítimo en el marco del bloque de constitucionalidad. Esto, en consideración a lo dispuesto por el artículo 3° de la Convención de Viena sobre Relaciones Diplomáticas de 1961, puesto que dentro de las funciones de las misiones diplomáticas se encuentran, entre otras, la de “b) proteger en el Estado receptor los intereses del Estado acreditante y los de sus nacionales, dentro de los límites permitidos por el derecho internacional”, situación que se asemeja a la de las Oficinas Consulares, en razón a lo previsto por el artículo 5° de la Convención de Viena sobre Relaciones Consulares de 1963. En tal sentido, es apenas comprensible que los Estados, en virtud de su soberanía y otras políticas internas como pueden ser el control demográfico o poblacional así como las relacionadas con la seguridad o la política criminal, tomen medidas y establezcan requisitos para admitir a ciudadanos extranjeros en su territorio con fines migratorios, esto es, con el propósito de generar un posible establecimiento allí mediante el otorgamiento de visas, residencia o nacionalidades, tal como lo explicaba la Cancillería en su respuesta. Asimismo, esta situación no constituye una circunstancia desconocida en términos locales, dado que el Gobierno de Colombia, de conformidad con el Decreto 2268 de 1995, tal como en otros países, tiene competencia discrecional para autorizar el ingreso de extranjeros e igualmente solicitar el certificado de antecedentes judiciales. Por esta misma razón, es que las autoridades migratorias del posible país receptor sí son terceros con un interés legítimo de conocer el registro de los antecedentes judiciales de un ciudadano sin lugar a supresiones

CERTIFICADO DE ANTECEDENTES JUDICIALES Y HABEAS DATA-Sentencia SU458/12 no es procedente para este caso

CERTIFICADO DE ANTECEDENTES JUDICIALES Y HABEAS DATA-No vulneración por cuanto solicitud por parte de gobierno extranjero con fines migratorios, obedece a fines legítimos

Referencia: Expediente T-4.516.485

Acción de tutela instaurada por Felipe[1] contra la Policía Nacional y los Ministerios de Defensa y del Exterior.

Magistrado Ponente:

LUIS GUILLERMO GUERRERO PÉREZ

Bogotá, D.C., doce (12) de febrero de dos mil quince (2015)

La Sala Tercera de Revisión de la Corte Constitucional, integrada por los magistrados Gabriel Eduardo Mendoza Martelo, Gloria Stella Ortiz Delgado y Luis Guillermo Guerrero Pérez, quien la preside, en ejercicio de sus competencias constitucionales y legales, ha proferido la siguiente

SENTENCIA

Dentro del proceso de revisión de los fallos proferidos, en primera instancia, por el Tribunal Administrativo de Cundinamarca- Sección 3, Subsección A- el 20 de mayo de 2014, y en segunda instancia, por el Consejo de Estado- Sección Cuarta- el 31 de julio de 2014, respecto de la acción de tutela presentada por Felipe contra la Policía Nacional y los Ministerios de Defensa

y del Exterior, solicitando la protección de sus derechos fundamentales al hábeas data y a la igualdad.[2]

I. ANTECEDENTES

El 7 de mayo de 2014, Felipe, obrando mediante apoderado judicial, presentó acción de tutela contra la Policía Nacional y los Ministerios de Defensa y del Exterior, pretendiendo que tales entidades ajusten, de conformidad con la sentencia SU-458 de 2012, los trámites de apostilla o legalización[3] del certificado de antecedentes judiciales bajo la leyenda “No tiene asuntos pendientes con las autoridades judiciales” tanto para aquellos que no han cometido delitos como para quienes habiéndolo hecho, la autoridad judicial competente haya decretado la extinción de la condena o la prescripción de la pena.

1.1. Hechos relevantes

Mediante providencia del 1 de octubre de 2003, el accionante fue condenado por el delito de peculado culposo a la pena principal de 18 meses de prisión y al pago de 30 S.M.L.M.V por el Juzgado 22 Penal del Circuito de Bogotá.[4]

EL 6 de agosto de 2008, el Juzgado 11 de Ejecución de Penas y Medidas de Seguridad comunicó al Departamento Administrativo de Seguridad (DAS), entidad que en ese entonces se encargaba del registro y la administración de antecedentes judiciales, que mediante providencia del 16 de julio del mismo año se había declarado la extinción de la condena al señor Felipe. Por ese motivo, le solicitaba a dicho Departamento y a los demás organismos de seguridad del Estado, la actualización y, en consecuencia, la cancelación de los antecedentes que figuraran por cuenta de la actuación penal llevada en contra del peticionario.[5]

De conformidad con la sentencia SU-458 de 2012, tras un derecho de petición, el accionante solicitó la actualización de sus antecedentes judiciales a la Dirección de Investigación Criminal e Interpol (DIJIN) de la Policía Nacional, la cual fue confirmada el 18 de febrero de 2014.[6]

En el año 2014, el peticionario adelantó un trámite de carácter migratorio, en compañía de su esposa y su hija menor de edad, ante la República Federativa de Brasil, con el fin de solicitar la visa de trabajo, para lo cual debió presentar su registro de antecedentes judiciales legalizado/apostillado y el de su esposa.[7] Aunque en la consulta de la plataforma en línea de la Policía Nacional el peticionario, según la SU-458 de 2012, “No tiene asuntos pendientes con las autoridades judiciales”, leyenda que de forma idéntica le aparece a su cónyuge, quien nunca ha sido condenada penalmente,[8] los certificados de antecedentes judiciales expedidos por la Cancillería en el trámite de apostilla y legalización hacen la respectiva diferenciación, puesto que mientras ella “No registra antecedentes judiciales de acuerdo con el art. 248 de la Constitución Política de Colombia”, él “No tiene asuntos pendientes con las autoridades judiciales”.

A su juicio, tal situación lo ubica en una posición de desigualdad frente a las personas que no tienen antecedentes judiciales, y en consecuencia, le impone una carga que, en últimas, le impediría llevar con éxito los trámites migratorios a otros países, en tanto terceros no autorizados por la sentencia SU- 458 de 2012, como otros Estados, podrían concluir que sí fue condenado penalmente, aun cuando la condena ya se había declarado extinta. Asimismo, afirma que suministrar información a otros Estados sobre la historia judicial de un ciudadano colombiano, cuando la misma excede la que reposa en la plataforma de consulta de la Policía Nacional según la sentencia de unificación citada, vulnera abiertamente su derecho al hábeas data y “(...) desde el punto de vista de la realidad social configura una extensión de la sanción”.

1.2. Solicitud

De acuerdo con los hechos anteriores, el peticionario solicitó al juez constitucional ordenar al Grupo de Consulta y Respuesta de Antecedentes de la Policía Nacional de Colombia la unificación de los certificados de antecedentes y requerimientos judiciales expedidos con motivo de trámites consulares, respecto de las personas que hubiesen tenido sanciones penales prescritas o extinguidas judicialmente y las personas que nunca hubieran cometido delitos, bajo una leyenda única y análoga para ambos grupos que señale, tal como lo hizo la SU-458 de 2012, que “No tiene[n] asuntos pendientes con las autoridades judiciales”, es decir, tal y como acontece con los certificados en línea a través del sitio www.policia.gov.co, link “antecedentes”.

Asimismo, con el fin de proteger sus derechos a la intimidad y al buen nombre, consagrados en el artículo 15 de la Constitución Política, el accionante le solicitó al juez de tutela la reserva de su nombre de todas las publicaciones procesales futuras, incluyendo las sentencias, tal como se realizó en la SU-458 de 2012.

1.3. Contestación de los accionados

1.3.1. Ministerio de Defensa Nacional, Dirección de Investigación Criminal e Interpol y Policía Nacional.

El 13 de marzo de 2014, el responsable de antecedentes judiciales de la Policía Nacional señaló que la entidad estaba dando pleno cumplimiento a los parámetros fijados por la Corte Constitucional en sentencia SU-458 de 2012 para la generación de antecedentes a través de la plataforma en línea dispuesta por la institución. Advirtió que en relación con los trámites de apostilla y legalización, la expedición del certificado de antecedentes judiciales se realiza a través de la página web del Ministerio de Relaciones Exteriores, procedimiento consular que no está a cargo de la Policía Nacional. En todo caso, destacó que la Dirección de Asuntos Migratorios, Consulares y Servicio al Ciudadano de dicho Ministerio, mediante Oficio No. 79524 del 27 de noviembre de 2012, comunicó que de conformidad con la SU-458 de 2012 el enunciado “No tiene asuntos pendientes con las autoridades judiciales” sólo es válido frente a particulares que no tengan interés legítimo, lo que no se cumple frente a las autoridades extranjeras, quienes en virtud de su soberanía, pueden ser considerados terceros con interés legítimo y en ese sentido, se les podría suministrar a plenitud la información fidedigna del pasado judicial.

1.3.2. Ministerio de Relaciones Exteriores- Cancillería.

Mediante oficio del 14 de mayo de 2012, el Director de Asuntos Migratorios, Consulares y Servicio al Ciudadano de la entidad aseguró que, de conformidad con el Decreto 3355 de 2009, el Ministerio de Relaciones Exteriores es el facultado legalmente para realizar el trámite de apostilla y legalización de un documento expedido electrónicamente, y **“(…) que lo que certifica es la firma del funcionario público en el ejercicio de sus funciones [mas] no el contenido ni la veracidad del mismo”**. (Subrayado original)

En ese sentido, precisó que el documento, cuya firma es apostillada o legalizada, “(…) proviene directamente de la base de datos de la POLICÍA NACIONAL y se genera por el sistema a la oficina de apostilla, lo que significa que va de entidad a entidad a través de la plataforma tecnológica y no es manipulado en modo alguno por los funcionarios de [la Cancillería], por ser únicamente la transmisión de datos e información que suministra la [institución policial].”

1.4. Decisiones objeto de Revisión

1.4.1. Sentencia de primera instancia

1.4.1.1. En primera instancia, mediante auto del 9 de mayo de 2014 por medio del cual se admitió la acción de tutela, el Tribunal Administrativo de Cundinamarca- Sección Tercera, Subsección A- desestimó la petición especial del accionante, relacionada con que se mantuviera en reserva su nombre de toda publicación procesal. Tal determinación se justificó en la medida en que los procesos judiciales, salvo las excepciones legales, eran públicos, por lo que prohibir la publicación de las sentencias o aplicar una reserva total del expediente, afectaría en forma desproporcionada el principio de publicidad. El Tribunal añadió que las reservas de nombres hechas por la Corte Constitucional en sus sentencias, solo procedían cuando la tutela versaba sobre aspectos que podían menoscabar en forma trascendental la intimidad, o cuando se involucraba a menores de edad, pacientes seropositivos, parejas del mismo sexo, información genética, entre otros.

1.4.1.2. Negada la petición especial y luego de recibidas las respuestas de las entidades demandadas, mediante providencia del 20 de mayo de 2014, el Tribunal resolvió negar el amparo de los derechos al hábeas data y a la igualdad reclamados por el accionante como vulnerados. Luego de hacer un desarrollo completo sobre las consideraciones de la sentencia SU-458 de 2012, señaló que, si bien el certificado de antecedentes judiciales del accionante es diferente al de su cónyuge, cuando en principio deberían contener la misma leyenda de conformidad con tal providencia, la expedición de dicho documento con fines de apostilla y legalización consular tiene una destinación especial, puesto que no es de acceso público ni está dirigido a terceros sin un interés legítimo, en tanto su solicitud está motivada por autoridades extranjeras, las cuales ostentan un propósito claramente definido en el ordenamiento jurídico con el fin de determinar los permisos de circulación en su territorio.

1.4.2. Impugnación

En la oportunidad procesal,[10] la parte demandante manifestó su desacuerdo con la decisión de primera instancia, reiterando los argumentos esbozados en el escrito de tutela y señalando que, a su juicio, el propósito distinto con el que se adelantaban los trámites consulares en este caso no constituía una razón suficiente ni admisible que justificara la diferenciación censurada, entre otras cosas, porque, (i) en estricto sentido, la información contenida en el certificado no la estaba suministrando el gobierno colombiano a un gobierno extranjero, sino que era el propio interesado el que aportaba el documento a efectos de adelantar la consecución de una visa y, adicionalmente, (ii) porque el acceso al certificado de antecedentes judiciales para trámites de apostilla o legalización es de relativa facilidad, tanto que cualquier persona lo podría obtener y no solamente el titular, pues la única limitante es la consignación bancaria de una tasa.

1.4.3. Sentencia de segunda instancia

1.4.3.1. Como cuestión previa, la Sección Cuarta del Consejo de Estado advirtió que la petición especial del accionante sobre la reserva de identidad debía ser estimada, en tanto, sus derechos al buen nombre y a la intimidad, así como los de su esposa, podrían verse expuestos o afectados, como quiera que a través de innumerables motores de búsqueda, las providencias judiciales ahora son de fácil acceso para terceros que no tiene intereses legítimos en el proceso. Asimismo, señaló que con acceder a dicha pretensión no se sacrifica el principio de publicidad, puesto que lo que se sometería a reserva serían los nombres del actor y de su esposa y no el proceso en sí

mismo, el cual deberá estar disponible en todas las bases de datos de la Rama Judicial.

1.4.3.2. Ahora, frente al problema jurídico de fondo, mediante providencia dictada el 31 de julio de 2014, el Consejo de Estado revocó la decisión de primera instancia con fundamento en que el formato utilizado para apostillar o legalizar los antecedentes judiciales del actor y de su esposa con fines migratorios permitía inferir la existencia de condenas penales en contra del primero, a pesar de encontrarse extintas, y en ese sentido, contrariaba la ratio decidendi de la SU-458 de 2012. De conformidad con esta misma providencia y con la Ley 1581 del mismo año, añadió que las autoridades extranjeras no eran terceros legitimados para conocer el pasado judicial completo de un ciudadano, puesto que solo podían acceder a dicha información (i) los titulares, sus causahabientes o representantes legales; (ii) las entidades públicas o administrativas en ejercicio de sus funciones legales o por orden judicial y; (iii) los terceros autorizados por el titular o por el legislador.

Con base en lo anterior, concedió el amparo del derecho al hábeas data del peticionario, y en consecuencia, ordenó que la leyenda de los certificados de antecedentes judiciales fuera unificada bajo “No tiene asuntos pendientes con las autoridades judiciales”, tanto para aquellas personas que no habían cometido delitos, como para quienes habiéndolo hecho, la condena se encontraba extinta o la pena había prescrito, tal como se había ordenado en la SU-458 de 2012. Asimismo, tal Corporación ordenó que “[la] leyenda deberá adoptarse, por igual, para los certificados de antecedentes judiciales que se expidan a cualquier persona, de tal forma que se garantice la protección efectiva del derecho al hábeas data de la parte actora.”

2. Actuaciones surtidas en sede de Revisión

2.1. Pruebas solicitadas, documentos e información allegada

2.1.1. Dado que para tomar una decisión en esta sede, se requería mayor información acerca del trámite consular adelantado por el demandante, así como múltiples aclaraciones sobre los pormenores de los procesos de apostilla y legalización de antecedentes judiciales ante la Cancillería, mediante Auto del 4 de febrero de 2015, el despacho del Magistrado Sustanciador estimó pertinente requerir tanto al peticionario como al Ministerio de Relaciones Exteriores en tal sentido.[11]

2.1.2. Mediante respuesta del 10 de febrero de 2015, el accionante aclaró que el certificado de antecedentes judiciales, tramitado ante la Cancillería para su apostillamiento o legalización, lo requería para solicitar una visa de trabajo ante el Consulado de la República Federativa del Brasil. Asimismo, señaló que el Consulado Brasileiro había aceptado los certificados de él y de su esposa, pese las redacciones diferentes.

2.1.3.1. Por su parte, la Cancillería Colombiana, mediante escrito recibido por la Secretaría de esta Corporación también el 10 de febrero de 2015, respondió a cada una de las inquietudes planteadas por el despacho del magistrado sustanciador. Frente al tema de los trámites consulares con fines migratorios y no migratorios, aclaró que los primeros se realizan con el propósito de adelantar, ante autoridades migratorias extranjeras, solicitudes de visa, de residencia o de nacionalidad, mientras que los segundos son aquellos que se realizan “(...) con un fin diferente a trámites de carácter migratorio”, es decir, todos los demás.

2.1.3.2. Asimismo, advirtió que dependiendo del fin migratorio o no de la solicitud, el contenido del certificado de antecedentes judiciales puede cambiar. Esta diferencia es explicada por la Cancillería mediante el siguiente comparativo:

La anterior diferencia en la expedición del certificado de antecedentes judiciales ante la Cancillería, se debe, y explica la entidad, “(...) a los graves perjuicios que sufrieron los colombianos residentes en el exterior, debido a la negativa de los gobiernos extranjeros de aceptar la leyenda “NO TIENE ASUNTOS PENDIENTES CON LAS AUTORIDADES JUDICIALES”, tanto para personas que no registran antecedentes, como para personas a quienes se haya decretado la extinción o prescripción de la pena. // Dicha leyenda condujo a las autoridades migratorias extranjeras a concluir que sí existen antecedentes penales en los solicitantes, y como consecuencia de lo anterior, a no convalidar la permanencia del connacional en territorio extranjero, negarle la visa, o la residencia o la nacionalidad.”

Subrayó que los países “(...) con los que principalmente se han presentado rechazos de solicitudes a los ciudadanos colombianos, debido a la leyenda “NO TIENE ASUNTOS PENDIENTES CON LAS AUTORIDADES JUDICIALES”, [han sido]: Argentina, Chile, España, Costa Rica, Ecuador, Brasil, Panamá, entre otros.”

Con fundamento en las anteriores dificultades y de conformidad con la SU- 458 de 2012, donde se resaltan los principios de finalidad legítima, necesidad, utilidad y circulación restringida de los datos, la entidad destacó que el contenido del certificado de antecedentes judiciales cuando se expide con finés migratorios no implica ninguna contravención del derecho al hábeas data por parte de la Cancillería.

2.1.3.3. Por otra parte, aclaró que no existe ninguna diferencia en el contenido del certificado de antecedentes judiciales apostillado/legalizado en función del país destinatario.

2.1.3.4. Frente a la pregunta de si, actualmente, el Ministerio de Relaciones Exteriores estaba habilitado para brindar información a países extranjeros sobre los antecedentes judiciales de un ciudadano colombiano por solicitud de aquellos, la Cancillería precisó, en primer lugar, que aunque el trámite de apostilla o legalización de Constancia de Antecedentes Penales se realizaba a través de la página web de dicho Ministerio, la Entidad que administraba la base de datos de antecedentes judiciales y expedía la respectiva constancia era la Policía Nacional, por lo que la Cancillería no tenía ningún tipo de acceso a la administración de tal información. Asimismo resaltó que el Ministerio de Relaciones Exteriores no entregaba información a ninguna autoridad extranjera, sino directamente al solicitante, quien era el que disponía de ella de acuerdo a su necesidad. Completó su respuesta, señalando que “(...) cuando un ciudadano al tramitar su Constancia de Antecedentes Penales “con fines migratorios”, le aparec[ía] la leyenda “NO TIENE ASUNTOS PENDIENTES CON LAS AUTORIDADES JUDICIALES”; las autoridades del respectivo país le solicita[ban] `ampliación de antecedentes´”, y para el efecto, el ciudadano debía hacer el requerimiento por escrito, solicitando la ampliación y autorizando la consulta de antecedentes para, posteriormente, recibir respuesta por la Policía Nacional. En todo caso, destacó que “[t]anto la solicitud como la respuesta [eran] canalizadas a través del Consulado, si el ciudadano así lo requ[ería].”

2.1.3.5. Con el propósito de establecer qué datos debían proporcionarse para tramitar la apostilla o legalización de los antecedentes judiciales y hasta qué punto la entidad garantizaba, a través de su sistema informático, que el titular era la única persona que podía obtener información sobre los mismos, el despacho del magistrado sustanciador solicitó a la entidad la aclaración de esta cuestión, frente a lo cual la Cancillería manifestó: “Si el ciudadano requiere Constancia de Antecedentes Penales “con fines no migratorios”, no se requiere ningún tipo de información.// Si el ciudadano requiere Constancia de Antecedentes Penales “con fines migratorios”, el sistema le

pide la confirmación de datos personales, que pueden ser:

Número de pasaporte y fecha de expedición del mismo, cuando se tiene pasaporte de lectura mecánica

Último trámite realizado a través del Sistema Integrado de Trámites al Ciudadano –SITAC-, y fecha de realización del mismo

A falta de alguno de los anteriores, el sistema le exige primero el registro, en el cual se deben indicar todos los datos personales y de localización del ciudadano.”

2.1.3.6. Ahora, frente a la forma en que la Cancillería estaba dando cumplimiento a la SU-458 de 2012, la entidad señaló que de conformidad con los principios de finalidad, necesidad, utilidad y circulación restringida desarrollados por dicha providencia, era posible expedir los certificados de antecedentes judiciales diferenciados, cuando se trataba de solicitudes con o sin fin migratorios. En todo caso, advirtió que aun cuando se justificaba la exposición del pasado judicial de una persona cuando se solicitaba el certificado con antecedentes judiciales con un fin migratorio, la Cancillería solo admitía que fuera el titular de la información quien, a través de su plataforma en línea, pudiera solicitar, obtener y disponer de la misma de acuerdo a su necesidad, tal como entregarla a una autoridad extranjera.

2.1.3.7. Por otra parte, la Cancillería señaló que las autoridades colombianas exigen el “certificado de antecedentes penales” como requisito para la solicitud de visa para residencia temporal MERCOSUR.[12] Y respecto a su leyenda, no se exige ninguna en especial; solo que sean claros los antecedentes reportados.

2.1.3.8. Frente a la ocurrencia de dificultades con motivo del cumplimiento de la sentencia SU-458 de 2012, la Cancillería señaló que se han presentado negación de visas, negación de solicitudes de residencia o nacionalidad y suspensión o aplazamiento de trámites de regularización de la situación migratoria de ciudadanos colombianos. De acuerdo con esta situación, y particularmente con relación a los efectos de la sentencia que ahora es objeto de revisión, emitida por la Sección Cuarta del Consejo de Estado, que en segunda instancia concedió el amparo en el caso estudiado y que generó un cambio estructural en toda la plataforma de apostillamiento y legalización, la Cancillería adjuntó copia de un documento con fecha del 11 de septiembre de 2014, en el que solicitaba al General Rodolfo Palomino, Director de la Policía Nacional, la búsqueda de una solución a las numerosas situaciones que se vienen presentando en los trámites migratorios adelantados por los connacionales en el país, así como en el exterior.

Dicho documento, anterior a la selección de este expediente, señala que a partir de la expedición del registro de antecedentes disciplinarios en los términos exigidos por la sentencia del Consejo de Estado, que ahora se revisa, se han generado gravísimas consecuencias para los ciudadanos colombianos frente a su permanencia en el extranjero (otorgamiento de residencia permanente en otros países o concesión de la nacionalidad por los mismos). Como antecedente de ello, citan al Director de Migración del Estado Argentino, Dr. Martín Arias Duval, quien informó que “(...) la leyenda “NO TIENE ASUNTOS PENDIENTES CON LAS AUTORIDADES JUDICIALES” no era satisfactoria para el Estado Argentino con miras a convalidar la permanencia migratoria del connacional que los solicite, requiriendo por el contrario una mayor precisión frente a aquellos ciudadanos colombianos que no tienen antecedentes judiciales con aquellos que relacionados a la misma leyenda presentan condenas cumplidas o extinguidas.” Con fundamento en ello, las

autoridades argentinas emitieron un comunicado donde informan a la comunidad colombiana que “para poder iniciar trámite de residencia, deberá[n] presentar certificado de antecedentes penales que acredite fehacientemente que no tiene[n] sentencia condenatoria anterior dictada a su respecto y que no registra[n] procesos penales en trámite”.

Por su parte, la Comunidad de Navarra (España) le negó la nacionalidad a un ciudadano colombiano con fundamento en la insuficiencia del contenido del certificado de antecedentes judiciales, así como el Consulado de Colombia en Madrid reportó una queja similar en el caso de otra ciudadana.[13] Advierte la Cancillería, que en poco más de un mes de notificada la sentencia, dicho Consulado ya había reportado más de 106 casos relacionados con la problemática señalada.

Otro de los ejemplos presentado por la entidad, es el del Departamento de Extranjería del Estado Chileno, quien sostiene que “la nueva lectura del antecedente “NO TIENE ASUNTOS PENDIENTES CON LAS AUTORIDADES JUDICIALES”, iguala a aquellas personas que NUNCA han tenido antecedentes con aquellas que tuvieron condena y ya cumplieron o la pena se ha extinguido, lo cual [para ellos] no es de recibo, por lo que se verán obligados a solicitar ampliación de los antecedentes judiciales a TODAS las personas que presenten el certificado con esa leyenda, decisión que acarrearía una nueva solicitud que toma un tiempo considerable y que a la postre podría resultar perjudicando a la persona interesada en la visa.”

Frente a dichas circunstancias, el Secretario General de la Cancillería presentó una solución en el marco de los principios desarrollados por la SU-458 de 2012 y le solicitó a la Policía Nacional la edificación de una base de datos de antecedentes judiciales con una finalidad y ámbito restringido, dirigido únicamente a formar parte de los trámites de carácter migratorio adelantados por ciudadanos colombianos con destino a autoridades de otros Estados. Esta base de datos, según dicha propuesta, solo podría ser consultada por el particular titular de la obligación, cuya identificación se garantizaría previa confirmación de datos de carácter personalísimo, como el número del pasaporte. Así mismo, le requirió a la institución para que las certificaciones expedidas con fines migratorios, contaran con el siguiente texto adicional: “La presente se expide únicamente para fines de carácter migratorio”, de conformidad con la sentencia SU- 458 del 21 de junio de 2012”.

De conformidad con lo observado por esta Sala, los parámetros de dicha propuesta hecha por la Cancillería a la Policía Nacional el 11 de septiembre de 2014, son los que vienen siendo empleados para la expedición de certificaciones en la actualidad.

2.1.4. Finalmente, al proceso se allegó un escrito recibido el 10 de septiembre de 2014 por la Secretaría de esta Corporación, en el que el Director de Asuntos Consulares, Migratorios y Servicio al Ciudadano de la Cancillería solicitaba a esta Corporación mediante “una alarmante petición” que el expediente de la referencia fuera seleccionado para revisión, reiterando “la magnitud del daño causado al proceso migratorio” con motivo de la sentencia del Consejo de Estado, que es precisamente la que la Corte revisa en esta oportunidad.

II. CONSIDERACIONES y fundamentos

1. Competencia

Esta Sala es competente para revisar la decisión proferida dentro del expediente de la referencia, con fundamento en los artículos 86 y 241 numeral 9° de la Constitución Política.

2. Planteamiento del caso, problema jurídico y esquema de resolución.

2.1. En el asunto sometido a Revisión, el señor Felipe presentó acción de tutela contra la Policía Nacional y los Ministerios de Defensa y del Exterior, tras considerar que tales entidades vulneraban sus derechos a la igualdad y al habeas data, al expedir su certificado de antecedentes judiciales con una leyenda que permite que terceros sin un interés legítimo- en este caso otros Estados- deduzcan que fue sentenciado penalmente a pesar de que su condena fue declarada extinta, contraviniendo, a su juicio, lo resuelto por esta Corporación en la SU-458 de 2012.

Las accionadas por su parte, particularmente la Cancillería, señalan que los parámetros de expedición del certificado de antecedentes judiciales cuando es con fines migratorios, dado que el peticionario buscaba obtener una visa de trabajo en otro país, no se rigen por las reglas desarrolladas en la citada sentencia de unificación. Lo anterior, como quiera que esta providencia lo que procuró fue salvaguardar el derecho al hábeas data de quienes habiendo sido condenados su pena había prescrito o la condena había sido declarada extinta, emitiendo una orden en el sentido de evitar que dicha información fuera revelada en forma indiscriminada a terceros sin ningún interés legítimo. En esa medida, a juicio de la Cancillería, los Estados sí son terceros con un interés legítimo de conocer el pasado judicial de un ciudadano extranjero que, en virtud de un trámite migratorio, solicita la autorización para circular en su territorio, motivo por el que no consideran que se hayan vulnerado los derechos del accionante.

En todo caso, la Cancillería señaló que la base de datos de antecedentes judiciales es de manejo exclusivo de la Policía Nacional, por lo que no tiene acceso a ella, y su única función es certificar, mediante el trámite de apostilla o legalización, la firma del funcionario que aparece en el documento, más no el contenido del mismo o su veracidad. Sin embargo, el responsable de antecedentes judiciales de la Policía Nacional, por su parte, indicó que en relación con los trámites de apostilla y legalización, la expedición del certificado de antecedentes judiciales se realizaba a través de la página web del Ministerio de Relaciones Exteriores, procedimiento consular que no estaba a cargo del cuerpo civil armado.

Frente a las decisiones judiciales que la Corte ahora revisa, el juez de primera instancia resolvió negar el amparo, formulando su motivación con base en lo expuesto por la Cancillería. No obstante, el Consejo de Estado, como juez de la impugnación, revocó la providencia, argumentando que el formato utilizado para apostillar o legalizar los antecedentes judiciales del actor y de su esposa con fines migratorios contrariaba la *ratio decidendi* de la SU-458 de 2012, puesto que permitía inferir la existencia de condenas penales en contra del primero, a pesar de encontrarse extintas. Asimismo, advirtió que de conformidad con el artículo 13 de la Ley 1581 de 2012, las autoridades extranjeras tampoco habían sido contempladas como terceros legitimados para conocer el pasado judicial completo de un ciudadano, por lo que ordenó que el contenido del certificado de antecedentes judiciales del actor con fines de apostilla o legalización fuera modificado de conformidad con la sentencia de unificación y además, dicho cambio se hiciera en todo el sistema de información.

Por su parte, la Cancillería expuso los diversos traumatismos que ha generado a todo el proceso migratorio dicha sentencia del Consejo de Estado. Señaló entre ellos, la no convalidación de la permanencia de ciudadanos colombianos en el extranjero, la negación de visas, residencia o nacionalidad, especialmente con las autoridades migratorias de Argentina, Chile, España, Costa Rica, Ecuador, Brasil y Panamá. Por tal situación, narró que había solicitado al Director de la Policía Nacional una solución al respecto, al tiempo que propuso la creación de dos bases de datos paralelas para la certificación de antecedentes judiciales, una con propósitos migratorios, y

otra sin dichos propósitos.

Finalmente, esta Sala tuvo conocimiento de que el Consulado de la República Federativa del Brasil aceptó los certificados del accionante y de su esposa, pese las redacciones diferentes.

2.2. En consideración a los antecedentes reseñados, corresponde a la Sala determinar si las entidades accionadas, comprometidas en el proceso de expedición del certificado de antecedentes judiciales apostillado o legalizado, vulneraron los derechos a la igualdad y al hábeas data del accionante, al no haber adoptado, en su caso y para trámites migratorios, la solución dada por la sentencia SU-458 de 2012 a la consulta de antecedentes judiciales, y en su lugar, haber diferenciado el contenido de dicho certificado para aquellas personas que lo requerían con el fin de solicitar a las autoridades de otro Estado permisos de migración a su territorio, incluyendo una leyenda que permitía inferir la existencia de condenas penales en su contra, a pesar de que las mismas se encontraran extintas o cuyas penas hubieran prescrito.

2.3. Con el propósito de responder a tal problema jurídico, esta Sala de Revisión se pronunciará sobre (i) el derecho al hábeas data, su justificación histórica y alcance en el ámbito nacional e internacional en la **protección de datos personales**; (ii) la evolución normativa del certificado de antecedentes judiciales, su naturaleza como dato personal protegible a través del hábeas data y efectos del amparo por la SU-458 de 2012; y (iii) la transferencia de datos personales entre Estados y sus límites de conformidad con el derecho interno y con los instrumentos de derecho internacional, para finalmente, resolver el caso concreto.

3. El derecho al hábeas data como justificación histórica del poder informático y su alcance en el ámbito nacional e internacional.

3.1. De acuerdo con las crecientes exigencias que en términos de información se han impuesto a los Estados para el desarrollo de sus políticas económicas, sociales, migratorias y criminales, solo por mencionar algunas, el manejo sistemático de datos personales ha encontrado mayores lugares comunes tanto a escala fronteriza como transfronteriza. Los procesos de distribución de bienes y servicios de orden público así como privado, la modernización en la gestión que adelantan las autoridades militares y de policía, o el fomento del funcionamiento del mercado, difícilmente podrían actuar en forma eficiente si no contaran con la posibilidad de acopiar, ordenar, utilizar y difundir datos personales.

3.1.1. Justamente, dichas posibilidades, acompañadas por copiosas plataformas tecnológicas que existen actualmente, permiten que los responsables de las bases donde se encuentran los datos[14] ostenten “un poder de facto, denominado “`poder informático””.[15] Dicho poder, mencionado por esta Corporación en la sentencia T-414 de 1992 como una especie de "dominio social sobre el individuo", y consistente en "la posibilidad de acumular informaciones en cantidad ilimitada, de confrontarlas y agregarlas entre sí, de hacerle un seguimiento en una memoria indefectible, de objetivizarlas y transmitir las como mercancía [en diversas formas]",[16] a aparejado numerosas ventajas al tiempo que riesgos.

3.1.2. La informatización del Estado y los consecuentes riesgos frente a la existencia de una “ingente masa de información”[17] también han conducido al manejo indiscriminado de los llamados datos personales, situación que, desde la segunda mitad del siglo pasado, empezó a ser considerada por la comunidad internacional[18] como potencial móvil de consecuencias nocivas frente al ejercicio de otros derechos humanos como la libertad, la identidad, la igualdad, la intimidad o el debido proceso.

3.1.3. La respuesta histórica del derecho internacional de los derechos humanos y del derecho constitucional a tal poder informático, fue la denominada autodeterminación informática o derecho de hábeas data;[19] nociones jurídicas que, a juicio de esta Corporación, han sido consideradas como equivalentes,[20] puesto que comparten un mismo referente, relativo a la libertad informática.

3.2. Con la vigencia de la actual Constitución, el hábeas data inició un proceso de reconocimiento como derecho autónomo, estando inicialmente subordinado al derecho a la intimidad,[21] para pasar luego a constituirse como una garantía esencialmente instrumental con alcances modestos[22] hasta convertirse en un derecho de amplio espectro.

3.2.1. A partir de la cláusula general del derecho a la libertad - artículo 16 constitucional- y la cláusula específica de libertad en el manejo de los datos- artículo 15 primer inciso- , la jurisprudencia de esta Corporación ha establecido la existencia-validez del llamado derecho a la autodeterminación informática como “[u]n derecho fundamental autónomo que tiene la función primordial de equilibrar el poder entre el sujeto concernido por el dato y aquél que tiene la capacidad de recolectarlo, almacenarlo, usarlo y transmitirlo”.[23]

3.2.2. En Colombia, el hábeas data está expresamente establecido en el artículo 15 de la Constitución Política de 1991, el cual, después de consagrar los derechos a la intimidad y al buen nombre, agrega que las personas: "De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas".

3.2.3. Particularmente, la construcción jurisprudencial sobre tal derecho ha permitido explorar con mayor detalle las tres facultades descritas en la disposición constitucional, aclarando que en virtud de la autodeterminación informática, el titular de los datos personales tiene la facultad de exigir a las administradoras de la información además, el acceso, inclusión, exclusión, corrección, adición, actualización, y certificación de los datos, así como la limitación en las posibilidades de divulgación, publicación o cesión de los mismos, de conformidad con los principios[24] que informan el proceso de administración de bases de datos personales, sobre los cuales esta Corporación se referirá más adelante.

3.3. Frente al objeto de protección del hábeas data, este Tribunal ha señalado que es en relación con el dato personal que este derecho cobra relevancia.[25]

En efecto, dada la naturaleza personal del dato, y por esta razón su considerable nivel de sensibilidad, las colisiones más significativas entre derechos, tales como el de información v.s. hábeas data, se generan precisamente porque la naturaleza del dato permite identificar al sujeto concernido: “El dato [personal] (...) constituye un elemento de la identidad de la persona, que en conjunto con otros datos sirve para identificarla a ella y solo a ella, y por lo tanto sería susceptible de usarse para coartarla, (...). Datos de este tipo [personales] serían sus señales particulares, relaciones de propiedad y de familia, aspectos de su personalidad, y señales de identidad de diversa índole que van emergiendo en las actividades de la vida. Todos estos datos combinados en un modelo, son equivalentes a una "huella digital" porque el individuo es identificable a través de ellos.”[26] En ese sentido, es posible observar que los datos impersonales, en principio, no son el objeto protegible del hábeas data, en tanto no permiten relacionar un individuo con la información existente.

3.3.1. Esta postura fue desarrollada con mayor precisión en la sentencia T-729 de 2002,

advirtiéndole que el dato objeto de protección por el hábeas data debía: “i) estar referido a aspectos exclusivos y propios de una persona natural, ii) permitir identificar a la persona, en mayor o menor medida, gracias a la visión de conjunto que se logre con el mismo y con otros datos; iii) su propiedad reside exclusivamente en el titular del mismo, situación que no se altera por su obtención por parte de un tercero de manera lícita o ilícita, y iv) su tratamiento está sometido a reglas especiales (principios) en lo relativo a su captación, administración y divulgación.”[27]

3.4. Así como la anterior tipología resulta necesaria para identificar el objeto protegible por el hábeas data, esta Corporación también ha considerado que existe una segunda gran tipología que necesariamente se superpone con aquella y que está relacionada con la clasificación de la información a partir de un criterio cualitativo en función de su publicidad y facilidad de acceso de acuerdo con las restricciones impuestas por el legislador.

3.4.1. Desde la sentencia T-729 de 2002, reiterada en este aspecto por la C-1011 de 2008, la jurisprudencia encontró cuatro grandes grupos: la información pública o de dominio público, la información semi-privada, la información privada y la información reservada o secreta. Adicionalmente, debe señalarse que esta clasificación también ha sido planteada para una mejor comprensión de la colisión entre los derechos a la información y al habeas data, en ocasiones extensible al derecho a la intimidad, en tanto contribuye a la delimitación e identificación tanto de las personas como de las autoridades que se encuentran legitimadas para acceder o divulgar información.[28]

3.4.1.1. En primer lugar, la información pública, calificada como tal según los mandatos de la ley o de la Constitución, puede ser obtenida y ofrecida sin reserva alguna y sin importar si se trata de información general o personal. En este grupo, pueden incluirse los actos normativos de carácter general, los documentos públicos en los términos del artículo 74 de la Constitución, y las providencias judiciales debidamente ejecutoriadas; así como los datos sobre el estado civil de las personas o sobre la conformación de la familia.

3.4.1.2. La información semi-privada, hace referencia a aquella de carácter personal o impersonal que no está contemplada en la categoría anterior y que para su acceso o conocimiento se requiere un grado mínimo de limitación. En ese sentido, la misma solo puede ser obtenida y ofrecida por orden de autoridad administrativa en el cumplimiento de sus funciones o en el marco de los principios de la administración de datos personales. Es el caso de los datos relativos a las relaciones con las entidades de la seguridad social o de los datos relativos al comportamiento financiero de las personas.

3.4.1.3. Por otra parte, la información privada puede tener contenidos personales o no y por encontrarse en un ámbito puramente privado, sólo puede ser obtenida y ofrecida por orden de autoridad judicial en el cumplimiento de sus funciones. Como ejemplos, se exponen los libros de los comerciantes, los documentos privados, las historias clínicas, los datos obtenidos en razón de la inspección a un domicilio o aquellos que se obtienen con posterioridad a la práctica de pruebas en procesos penales sujetos a reserva.

En efecto, encuentra la Sala que la información sobre antecedentes judiciales puede ser calificada en ocasiones como pública, pero también como semi-privada y privada al mismo tiempo. Esta oscilación se debe a que, en algunos casos es posible conocer el certificado de antecedentes penales de cualquier persona aportando únicamente su número de cédula tal como sucede con la plataforma de consulta de la Policía Nacional, pero entendiendo que los datos arrojados por la misma no ofrecen toda la historia judicial de una persona y que el acceso a dicha información

completa está sometido a la observancia de una serie de principios que orientan la administración de datos personales y que hacen que, en últimas, el contenido de un documento de tal naturaleza solo pueda ser obtenido, administrado y difundido por su titular o por un tercero con un interés legítimo constitucional o legalmente reconocido. Este tema en particular será tratado en los siguientes capítulos.

3.4.1.4. Finalmente, se tiene la información reservada que, por tener carácter exclusivamente personal y por su estrecha relación con los derechos fundamentales del titular - dignidad, intimidad y libertad-, se encuentra reservada a su órbita y no puede ser obtenida ni ofrecida ni siquiera por autoridad judicial en el cumplimiento de sus funciones. Como ejemplos de ello se tiene la información genética, y los llamados "datos sensibles"[29] o relacionados con la ideología, la inclinación sexual o los hábitos de la persona.

3.5. Especialmente, la solución a los conflictos generados en relación con la información semi-privada y privada, que es frente a la cual se generan mayores incertidumbres de acopio y divulgación, se encuentra gobernada por los principios que informan el proceso de administración de bases de datos personales. Tal como se vio, el derecho a la autodeterminación informática, tiene dos dimensiones distintas al tiempo que complementarias. De un lado, le confiere al titular de los datos el poder jurídico para conocer e incidir sobre el contenido y la difusión de los mismos. Y por otro, insta un conjunto de directrices a partir de las cuales, los responsables de las bases de datos, deben reordenar todo el proceso de acopio, uso y transmisión de datos personales. Esta segunda dimensión, está compuesta por los anunciados principios y no es otra cosa que el producto de las tensiones que la Corte, desde sus fallos más tempranos, ha identificado entre la preservación del hábeas data, la intimidad, la información y, en menor medida, el derecho al buen nombre.

3.5.1. Particularmente, la especial necesidad de disponibilidad de información mediante la conformación de bases de datos personales colisiona con el requerimiento de proteger las facultades que el hábeas data le confiere a sus titulares frente a los posibles riesgos del proceso de administración de datos. En ese sentido, con el fin de garantizar la armonía entre dichos bienes jurídicos, los principios sobre administración de datos han surgido como una alternativa instrumental de orden argumentativo y de reentendimiento sobre las facultades otorgadas por el Constituyente en el artículo 15 superior, así como de las responsabilidades impuestas a los administradores y usuarios de la información.

3.5.2. Aunque posteriormente el legislador colombiano incorporaría al ordenamiento algunos de ellos a través de la leyes 1266 de 2008 y 1581 de 2012, desde el año 1994, la Corte empezó a desarrollar una serie de directrices aplicables a la interpretación y solución de dichos conflictos, las cuales fueron sistematizadas en la sentencia T-729 de 2002 en los principios de libertad, necesidad, veracidad, integridad, incorporación, finalidad, utilidad, circulación restringida, caducidad e individualidad. En consideración al problema jurídico en concreto que la Sala debe resolver, no serán desarrollados todos los mencionados principios, sino solo aquellos que resultan pertinentes para el propósito de esta providencia.

3.5.2.1. En la sentencia T-022 de 1993, se exploró por primera vez el principio de libertad.[31] En virtud del mismo, se estableció que los datos personales sólo pueden ser registrados y divulgados con el consentimiento libre, previo y expreso del titular.[32] Este Tribunal ha relacionado este principio con la prohibición de obtención y tratamiento de información adquirida de manera ilícita, de tal forma que se encuentra prohibido el manejo y divulgación de dichos datos, sin la previa autorización del titular o de sus representantes.

3.5.2.2. Por su parte, el principio de necesidad, establece que los datos personales registrados deben ser los estrictamente necesarios para el cumplimiento de las finalidades perseguidas con la base de datos. En ese sentido, se encuentra prohibido el registro y divulgación de datos que no guarden estrecha relación con el objetivo de la base de datos a la que pertenecen o pretenden hacerlo.

3.5.2.3. Por su parte, sobre el principio de finalidad, la Corte ha manifestado que el suministro de datos personales debe realizarse en un contexto más o menos delimitado, es decir, que “la referida información [debe destinarse] a realizar los fines exclusivos para los cuales fue entregada por el titular, en relación con el objeto de la base de datos y con el contexto en el cual estos son suministrados”. Por lo tanto, según este principio “tanto el acopio, el procesamiento y la divulgación de los datos personales, debe obedecer a una finalidad constitucionalmente legítima, definida de manera clara, suficiente y previa; de tal forma que queda prohibida la recopilación de datos sin la clara especificación acerca de la finalidad de los mismos, así como el uso o divulgación de datos para una finalidad diferente a la inicialmente prevista.”[34]

De acuerdo con lo anterior entonces, el principio de finalidad impone una triple lectura sobre el tratamiento de los datos. En primer lugar, deben ser procesados con un propósito específico y explícito; así mismo la finalidad de su recolección debe ser legítima a la luz de las disposiciones constitucionales; y finalmente, deben estar destinados a un fin exclusivo.

3.5.2.4. Como corolario del principio de finalidad, se encuentra el de utilidad. En virtud de éste, la ausencia de una función clara del tratamiento sobre un dato constituye un abuso del derecho. En este sentido, en la sentencia T-119 de 1995 se expresó que “(...) la sola autorización de funcionamiento de las entidades administradoras de datos, no constituía garantía de la legitimidad de sus conductas”. En consecuencia, tanto el acopio, el procesamiento y la divulgación de los datos personales, “debe cumplir una función determinada, como expresión del ejercicio legítimo del derecho a la administración de los mismos; por ello, está prohibida la divulgación de datos que, al carecer de función, no obedezca a una utilidad clara o determinable.”

3.5.2.5. En quinto lugar, el principio de acceso y circulación restringida, demanda que “la divulgación y circulación de la información est[én] sometid[as] a los límites específicos determinados por el objeto de la base de datos, por la autorización del titular y por el principio de finalidad, de tal forma que queda prohibida la divulgación indiscriminada de los datos personales”.[35]

En este sentido, el tratamiento de los datos solo puede adelantarse, en general, por el propio titular, o las que personas que le representen o el que el legislador autorice. Asimismo, este principio es el que restringe que los datos personales, salvo información pública, se encuentren disponibles en plataformas abiertas o de libre acceso como Internet, a menos que se ofrezca un control técnico para asegurar permisos limitados.

3.6. Si bien el anterior derrotero sobre principios obedece a una construcción jurisprudencial de este Tribunal, el precedente citado recoge, en gran medida, la tendencia internacional de establecer principios de administración de datos personales que sirvan de sustento para la protección de los derechos fundamentales de los sujetos concernidos, en especial la intimidad y el hábeas data.

3.6.1. En efecto, esta compatibilidad se hace visible frente al Sistema Universal de Protección de

Derechos Humanos, así como frente al Sistema Interamericano, a través de instrumentos como la Observación General No. 16, interpretativa del artículo 17 del Pacto Internacional de Derechos Civiles y Políticos[36] y otros, como el Informe Anual de la Relatoría para la Libertad de expresión CIDH[37] o los preparativos para el Proyecto de principios y recomendaciones preliminares sobre la protección de datos.

3.6.2. Asimismo, dicho precedente jurisprudencial también ha resultado afín a otros estándares internacionales en materia de principios que rigen el derecho a la autodeterminación informática. En este sentido, es posible identificar el Convenio No. 108 del 28 de agosto de 1981 del Sistema de Protección Europeo, que fue uno de los primeros en instar a los miembros de la Comunidad a adoptar en sus legislaciones internas unos principios mínimos de protección, ante el surgimiento de las grandes bases de información que podían poner en riesgo los derechos de los ciudadanos.[39]

Posteriormente, fueron adoptados otros instrumentos internacionales como la Resolución 45/95 del 14 de diciembre de 1990[40] y la Directiva 95/46/CE, el primero por el Consejo de la Unión de la Organización de las Naciones Unidas y la segunda por el Parlamento Europeo.

3.6.3. Finalmente, con base en los documentos expedidos tanto a nivel de la Unión Europea como los generados en el entorno regional, la Organización de los Estados Americanos diseñó un catálogo de 15 directrices, las cuales definió como “la base de la legislación sobre protección de datos en todo el mundo y que podrían servir de base para un instrumento internacional o una legislación modelo sobre protección de datos”. Entre aquellos que relaciona, se encuentran los principios **de legitimidad y justicia;**[42] **el de propósito específico, de limitación y necesidad;**[43] **el de transparencia;**[44] **el de rendición de cuentas;**[45] **el de condiciones para el procesamiento de datos;**[46] **el de la revelación de información a los procesadores de datos;**[47] **aquél sobre las transferencias internacionales de datos;**[48] **el relativo al derecho a la persona al acceso a la información;**[49] **el derecho de la persona para corregir y suprimir sus datos personales;**[50] **el principio de garantía a objetar el procesamiento de datos personales;**[51] **el principio sobre medidas de seguridad para proteger los datos personales;**[52] **el de la confidencialidad;**[53] y **el principio de control, cumplimiento y responsabilidad en el manejo de datos por parte del operador o principio de autoridad independiente que garantice la aplicación de la normatividad.**

3.6.4. Frente a lo anterior, esta Corporación observa que los distintos sistemas de protección de derechos, tanto el universal, como los regionales, instan a los Estados a establecer en sus ordenamientos jurídicos unos principios mínimos que han de regir el manejo de la información de datos; estándares que, en su mayoría y aunque de diversas formas, se encuentran incorporados a la jurisprudencia de esta Corporación y al ordenamiento legal.

3.7. Precisamente, en relación con la incorporación de dichos principios en desarrollos legislativos, el 17 de octubre de 2012 fue expedida la Ley Estatutaria 1581, **“Por la cual se dictan disposiciones generales para la protección de datos personales”**. El artículo 4º de dicha ley, establece los principios de legalidad en materia de tratamiento de datos, el de finalidad, de libertad, de veracidad o calidad, de transparencia, de acceso y circulación restringida, de seguridad y el principio de confidencialidad. Aunque dichos principios no se corresponden en su totalidad con los que la jurisprudencia constitucional ha desarrollado, en Sentencia C-748 de 2011, esta Corporación advirtió que “(...) la enunciación de estos principios no puede entenderse como la negación de otros que integren o lleguen a integrar el contenido del derecho fundamental al habeas data”, siempre que sean compatibles con las disposiciones constitucionales en estricto

sentido, así como con las normas internacionales que han desarrollado la materia.[55]

3.8. Finalmente, además de los principios enunciados expresamente por la Ley Estatutaria de Protección de Datos Personales, mediante la misma sentencia que analiza su constitucionalidad, la C-748 de 2011, este Tribunal interpretó que existían otros principios derivados de su núcleo temático que, a pesar de no encontrarse numerados en el artículo 4, se entendían incorporados en razón de una lectura sistemática del entonces proyecto de Ley Estatutaria, entre ellos, el principio de exigencia de estándares de protección equivalentes para la transferencia internacional de datos, que “(...) tal y como se deduce del artículo 26 del Proyecto de Ley Estatutaria, existe una prohibición de transferencia internacional a cualquier tipo de países que no proporcionen niveles adecuados de protección de datos.”

3.9. Si bien la Ley Estatutaria de Protección de Datos Personales establece algunas excepciones de aplicación para ciertos temas y en ese sentido podría considerarse que la legislación colombiana en materia de hábeas data es de tipo sectorial,[56] es decir que las regulaciones son distintas en virtud del tipo de dato personal de que se trate, a partir de sentencias como la C-1011 de 2008 y la C-748 de 2011, dicha conclusión solo podría ser parcial, como quiera que las mismas normas de la ley estatutaria, en cuanto prevén los principios de administración de datos personales, al igual que los derechos y deberes de titulares, fuentes y usuarios; son parámetro común para la evaluación de legitimidad de todas las modalidades de tratamiento de información personal, incluidos las relacionadas con antecedentes judiciales.

4. La evolución normativa del certificado de antecedentes judiciales, su naturaleza como dato personal protegible a través del hábeas data y efectos del amparo por la SU-458 de 2012.

4.1. El certificado de antecedentes judiciales tiene su origen en el certificado de identidad personal regulado por el Decreto 884 de 1944. Inicialmente, este documento era expedido por las oficinas de identificación personal de la Policía Nacional y acreditaba que su portador no había cometido delitos contra el Tesoro Público ni contra la propiedad particular. Adicionalmente, su presentación era indispensable para tomar posesión de cualquier empleo nacional, departamental o municipal. [58]

Años después, luego de la creación del Departamento Administrativo de Seguridad- DAS-, [59] por medio de la Ley 15 de 1968 el Congreso autorizó al Gobierno Nacional para determinar, por intermedio del DAS, lo relacionado con las características, especificaciones, vigencias, uso y valor de adquisición de las cédulas de extranjería y los certificados de conducta. Posteriormente, el artículo 10 de la Ley 4ª de 1981 [60] ratificó la autorización conferida al Gobierno Nacional para reglamentar lo relacionado con los modelos de las cédulas de extranjería, certificados judiciales y carnés mencionados en dicha ley.

Ulteriormente, el Decreto 2110 de 1992, en su artículo 6º, precisó que era función del DAS “[a]uxiliar a las autoridades judiciales y administrativas en las diversas ramas de la criminalística, llevar los registros delictivos y de identificación y expedir los certificados judiciales y de policía.” Asimismo, se reguló esta misma función en cabeza de dicha entidad mediante el Decreto 218 de 2000, [61] por medio del cual se modificó la estructura del organismo de seguridad.

En cumplimiento de la misma obligación, por medio del artículo 2º numeral 12 del Decreto 643 de 2004, se siguió confiando al DAS la competencia de “llevar los registros delictivos y de

identificación nacionales, y expedir el certificado judicial”. A su vez, en el artículo 3º del Decreto 3738 de 2003, “por el cual se dictan normas sobre reseña delictiva y expedición de Certificados Judiciales”, se le otorgó al mismo organismo el deber de mantener y actualizar los “registros delictivos y de identificación nacionales de acuerdo con los informes y avisos que para el efecto deberán remitirle las autoridades judiciales, conforme a la Constitución Política y la ley”.

4.2. No obstante, el DAS fue suprimido por mandato del artículo 1º del Decreto 4057 de 2011.

A su vez, mediante el artículo 3 numeral 3.3, del mismo Decreto, la función de “llevar los registros delictivos (...) y expedir los certificados judiciales (...)” fue transferida al Ministerio de Defensa-Policía Nacional. En forma paralela, mediante el artículo 2º del Decreto 0233 del 2012, “por medio del cual se modifica la estructura del Ministerio de Defensa”, se le confiaron a la Dirección de Investigación Criminal e INTERPOL de la Policía Nacional distintas funciones relacionadas con la administración de la base de datos personales sobre antecedentes penales (organizar, actualizar y conservar los registros, implementar mecanismos de consulta en línea, garantizar la seguridad de los registros, entre otros).[62]

4.3. Frente al contenido del certificado de antecedentes judiciales, esta Corporación ha señalado que se trata de “(...) un documento (...), en el cual se certifica la situación judicial de un ciudadano frente a la justicia y autoridades colombianas. Estipula si el titular no tiene asuntos pendientes con las autoridades judiciales y de policía, o si no es solicitado por las mismas autoridades”[63].

4.3.1. Justamente, en la medida que dichos datos asocian una situación determinada (haber sido condenado penalmente por una autoridad judicial competente) con una persona natural, es que la Corte ha considerado que los antecedentes judiciales tiene el carácter de datos personales. En efecto, esta información es propia y exclusiva de la persona, y permiten identificarla, reconocerla o singularizarla en mayor o menor medida, de forma individual o en conexión con otros datos personales.[64] Es decir que por su naturaleza de dato personal, el registro sobre antecedentes judiciales es objeto de protección constitucional a través del hábeas data.

En consonancia con esto, la Corte ha catalogado además a los antecedentes judiciales como el dato negativo por excelencia,[65] puesto que, facilitan la relación de circunstancias “no queridas, perjudiciales, socialmente reprobadas o simplemente desfavorables” con una persona natural, cuestión que problematiza aún más los conflictos entre hábeas data y derecho a la información, en tanto se “asocia el nombre de una persona con la ruptura del pacto social, con la defraudación de las expectativas normativas o con la violación de los bienes jurídicos fundamentales.”

4.3.2. No obstante la alta sensibilidad que generan al ser el dato negativo por excelencia, los antecedentes judiciales cumplen importantes funciones amparadas por el ordenamiento jurídico. En materia penal, sirven para constatar la procedencia de algunos subrogados penales, para determinar la punibilidad, y para establecer si las personas privadas de la libertad que solicitan un beneficio administrativo, tienen o no requerimientos pendientes con otras autoridades judiciales.[67] Adicionalmente, los antecedentes penales permiten establecer la existencia de inhabilidades; sirven entonces a la protección de los intereses generales y de la moralidad pública.[68] Asimismo, el registro de antecedentes penales es empleado por autoridades judiciales y con funciones de policía judicial, para el cumplimiento de sus funciones relacionadas con la persecución del delito y con labores de inteligencia asociadas a la seguridad nacional.[69] En el mismo sentido, esta Corporación mediante providencia C-536 de 2006, agregó otra serie de asuntos para los que se requería el certificado de antecedentes judiciales, tales como la tenencia o

porte de armas de fuego;[70] para recuperar la nacionalidad colombiana de quienes hubieren sido nacionales por adopción;[71] para la adopción de menores de edad;[72] o para el trámite de visa siempre y cuando fuera solicitado por la respectiva embajada, entre otros.

4.3.3. Considerando entonces la importancia que tienen las bases de datos relacionadas con antecedentes judiciales en el marco del Estado Constitucional y que su existencia obedece a legítimos fines de la misma estirpe, esta Corte ha señalado que su registro no puede ser considerado como una sanción. En efecto, si bien los antecedentes penales son el producto de la imposición de un castigo, no son la pena en sí misma ni adquieren autonomía punitiva.[73]

4.4. En todo caso, lo anterior no quiere decir que la información sobre antecedentes judiciales no pueda ser suprimida de forma relativa de acuerdo con la conciliación de varios elementos normativos que concurren en el caso de la administración de información personal en esta materia. En relación con este tema, la Sentencia de Unificación 458 de 2012 se encargó de plantear y resolver, a partir de los principios desarrollados en el capítulo anterior, los casos de diversas personas que argumentaban que, pese a que su pena había prescrito o se había declarado la extinción de la condena, en sus certificados, los cuales estaban a disposición de cualquier persona, figuraba una leyenda que permitía inferir que contra ellos se había dictado una sentencia penal, situación que estimulaba escenarios de discriminación laboral.

4.4.1. En razón de las importantes funciones que cumplen los antecedentes judiciales tal como se vio, la Corte advirtió en aquella oportunidad que la supresión total de los mismos no era una alternativa viable desde el punto de vista constitucional: “Ya lo vimos al referir el caso de las inhabilidades intemporales de carácter constitucional, las especiales funciones que en materia penal cumple la administración de esta información personal, así como sus usos legítimos en materia de inteligencia, ejecución de la ley y control migratorio. En estos casos, la finalidad de la administración de esta información es constitucional y su uso, para esas específicas finalidades, está protegido además por el propio régimen del habeas data.”

4.4.2. Sin embargo, señaló que, en virtud de los principios sobre administración de datos personales, los titulares de los mismos se encuentran facultados para ejercer la facultad de supresión relativa frente a la circulación irrestricta de la información sobre antecedentes judiciales cuando el propósito de su divulgación no reporte una clara finalidad, necesidad y utilidad constitucional: “Sin embargo, cuando la administración de la información personal relacionada con antecedentes pierde conexión con tales finalidades deja de ser necesaria para la cumplida ejecución de las mismas, y no reporta una clara utilidad constitucional; por tanto, el interés protegido en su administración pierde vigor frente al interés del titular de tal información personal. En tales casos, la circulación indiscriminada de la información, desligada de fines constitucionales precisos, con el agravante de consistir en información negativa, y con el potencial que detenta para engendrar discriminación y limitaciones no orgánicas a las libertades, habilita al sujeto concernido para que en ejercicio de su derecho al habeas data solicite la supresión relativa de la misma.”

En efecto, aclaró esta Corporación, si bien ciertas finalidades legítimas impiden que opere una supresión total del dato, ello no significa que la facultad de supresión relativa, en cabeza del titular del mismo, también desaparezca. Se precisó que ésta última facultad cobra trascendencia frente a la publicidad indiscriminada de la información sobre antecedentes penales cuando la misma no cumple una finalidad legal o constitucional, no es útil o necesaria. Adicionalmente este Tribunal señaló que no todas las personas son terceros con un interés legítimo en dicha información y que facilitar un incontrolado acceso al poder informático sobre los antecedentes

judiciales, no solo no observa los principios sobre administración de datos personales, sino que además puede constituir una barrera de facto para el ejercicio de otros derechos, como ocurrió con los casos estudiados por la SU, relacionados con el acceso al derecho al trabajo y su conservación.

4.4.3. Con fundamento en ello, la Corte advirtió que “(...) cualquier función que esté llamada a cumplir esta base de datos [la de antecedentes penales] debe ser conforme con una finalidad clara, expresa, previa y legítima definida en la ley. [Por tal motivo], frente a las funciones del certificado de antecedentes traídas a colación, la Corte nota que todas están reconocidas en normas de derecho positivo vigente, ligadas a un trámite específico, adelantado ante autoridad competente y cuya finalidad en principio está determinada de manera clara y precisa.” A lo que **agregó que la función del “(...) control migratorio adelantado por autoridades de otros Estados (...), [también tenía] un ámbito restringido y una finalidad más o menos precisa (...).** Y que, “(...) por el contrario, (...) en aquellos casos [en] que el certificado [era] exigido por particulares, con el objeto de celebrar contrato laboral o de prestación de servicios, las funciones del [mismo] y las finalidades que se persigu[ían] con su circulación, no [eran] claras ni precisas, [ni tampoco estaban] soportadas en una norma de derecho positivo.” (Subrayado y negrita fuera del original)

4.4.4. En ese sentido, este Tribunal concluyó que la conducta del administrador de la base de datos sobre antecedentes penales que en dichos casos había permitido que terceros tuvieran acceso indiscriminado, inorgánico y no acorde con una finalidad clara y precisa establecida en la Constitución o la Ley a dicha información personal, había vulnerado el derecho al hábeas data de los accionantes. Por tal motivo, ordenó a la Policía Nacional que al momento de facilitar el acceso a la base de datos impidiera que terceros sin un interés legítimo pudieran conocer o inferir la existencia de antecedentes penales de aquellas personas, que ya habían cumplido la condena, o cuya pena se encontraba prescrita, motivo por el que la leyenda de los certificados de estas personas así como para las que nunca hubieran cometido delito debía rezar “no tiene asuntos pendientes con las autoridades judiciales”.

Por este motivo, la Sala observa que la ratio decidendi de la SU-458 de 2012 no implica que todas las bases de datos sobre antecedentes judiciales deban gobernarse por la misma solución que en dicha oportunidad se dio a la consulta de los registros que administra la Policía Nacional, puesto que esta decisión fue adoptada en consideración a que, tratándose de una plataforma de libre acceso, no todas las personas que la consultaban aguardaban consigo un interés legítimo y por lo tanto, en estos casos no se cumplía con el principio de finalidad. En ese sentido, es claro para la Corte que, a partir de dicha providencia, pueden existir otras bases de datos sobre antecedentes delictivos que, en virtud de su finalidad y acceso restringido- solo por el titular o terceros con un interés legítimo-, puedan arrojar información que permita inferir la existencia de antecedentes penales. En otras palabras, la protección al hábeas data ofrecida por la SU-458 de 2012 es exclusivamente para evitar que determinadas personas, esto es, terceros sin ningún interés legítimo tengan acceso indiscriminado al pasado judicial de un ciudadano.

5. Principio de exigencia de estándares de protección equivalentes para la transferencia internacional de datos.

5.1. Tal y como lo reseñó esta Corporación en la sentencia C-748 de 2011 y como se indicó en el capítulo 3 de esta providencia, del artículo 26 de la Ley Estatutaria de Protección de Datos Personales, se deduce una prohibición de transferencia internacional a cualquier tipo de países que no proporcionen niveles adecuados de protección de datos.[74]

5.2. La transferencia internacional de datos personales ha surgido como consecuencia de la globalización y los fenómenos de integración económica y social, en los que tanto las empresas como las entidades gubernamentales requieren transferir datos personales destinados a diferentes propósitos. Por motivos de seguridad pública, seguridad nacional, investigaciones contra el terrorismo, labores de inteligencia militar o policial, cooperación judicial o controles de inmigración, los Estados se han visto en la necesidad de disponer reglas que deben observarse con miras a que los esfuerzos internos de protección informática de cada país no sean inútiles al momento de su exportación a otros países.[75]

5.3. En complemento a lo establecido en el capítulo 3 de esta sentencia, Europa ha sido considerada pionera en establecer fórmulas jurídicas tendientes a la protección de datos cuando se transfieren a terceros países. Así, uno de los presupuestos exigidos para que se pueda realizar la transferencia es que el país receptor cuente con un adecuado nivel de protección a la luz del estándar europeo.[76] De acuerdo con el Profesor Remolina Angarita, dicho nivel se refiere a que el Estado importador tenga un grado de protección superior, igual, similar o equivalente al del Estado exportador, dándole aplicación al principio de continuidad en la protección de datos.

5.4. De esta manera, el Grupo de Protección de las Personas en lo que respecta al Tratamiento de Datos Personales[78], en el marco de la Comisión Europea adoptó dos documentos de importancia: Las primeras orientaciones sobre la transferencia de datos personales a países terceros: posibles formas de evaluar la adecuación (Bruselas, 1997) y, transferencias de datos personales a terceros países: aplicación de los artículos 25 y 26 de la Directiva sobre protección de datos de la UE (Bruselas 1998.)

5.4.1. En consideración a que los países no tienen un régimen de protección de datos uniforme, el mencionado Grupo a partir de lo contenido en la Directiva 95/46/CE, el Convenio 108 de 1981, las directrices de la Organización para la Cooperación y el Desarrollo Económico OCDE de 1980 y los principios de la ONU de 1990, ya citados, fijó una serie de principios comunes para determinar si las normas de un país específico brindaban un nivel adecuado de protección. Según dicho estándar, los principios mínimos que deben informar los procesos de transferencias de datos hacia el extranjero deben contemplar la limitación de la finalidad; la calidad de los datos y proporcionalidad; la transparencia; la seguridad; el acceso, rectificación y oposición; las restricciones a las transferencias sucesivas a otros países y; las disposiciones sectoriales o adicionales para el tratamiento de datos de tipo especial donde se incluye, datos sensibles, mercadeo directo y decisión individual automatizada.[79]

5.4.2. Bajo dichos instrumentos, se entiende entonces que, un país cuenta con un nivel adecuado de protección de datos personales, si (i) consagra una norma general sobre protección de datos personales que incorpore los principios mínimos mencionados que abarquen los derechos de los actores en el proceso del tratamiento informático así como ciertas cualidades del dato, además de (ii) las disposiciones sectoriales o adicionales que deben rodear el tratamiento de esa información.[80]

5.5. Con todo, debe recordarse que el mismo artículo 26 de la Ley Estatutaria de Protección de Datos Personales crea, por otra parte, un conjunto de excepciones a la regla general que prohíbe la transferencia de datos personales a un país tercero que no garantice un nivel de protección adecuado. Es decir, permite la transferencia de datos a países que pueden no garantizar un nivel adecuado de protección, en casos como el que nos concierne, en que el titular de la información ha “(...) otorgado su autorización expresa e inequívoca para la transferencia.”

5.5.1. Frente a esta excepción, la propia Corte en la sentencia C- 748 de 2011, manifestó que no se percibía inconveniente alguno en cuanto a su constitucionalidad, puesto que para su procedencia se prescribe la autorización expresa e inequívoca del titular del dato, lo que en efecto ocurre, en desarrollo del principio de la libre voluntad del titular de autorizar la circulación de la información. “Por lo tanto, es claro que aunque se permite la transferencia de datos a un país que no brinda estándares de protección adecuados, la misma se realiza bajo la responsabilidad de su titular.”

5.6. En ese orden de ideas, se entiende que la exigencia de estándares de protección equivalentes para la transferencia internacional de datos, tal como se explicó al final del capítulo 3, es una pauta que por su vocación principialística no solamente puede aplicarse en forma sectorial o a un tipo específico de bases de datos pese a que la legislación colombiana en materia de hábeas data ostente dicho carácter, sino que es de aplicación común y en ese sentido, tal principio, como sus excepciones constituyen herramientas para la solución de casos en los que se hallen involucradas bases de datos relacionadas con antecedentes judiciales. En efecto, encuentra la Corte que dicha excepción al principio de transferencia de datos referida en el párrafo anterior, constituye por sí misma la expresión de otro principio, el de libertad. En ese sentido, se entiende que dicha excepción, relacionada con la voluntad del titular para dar a conocer información personal a un tercero por él indicado, en este caso su registro de antecedentes judiciales a otro Estado, es plenamente admisible de conformidad con el entendimiento jurisprudencial sobre la aplicación principialística de la Ley 1581 de 2012, particularmente en lo que hace al principio de libertad en la administración de datos personales.

5. Análisis del caso concreto

5.1. Habiendo la Sala analizado la decisión de unificación del año 2012, es posible concluir que las entidades responsables en el manejo de los antecedentes judiciales del señor Felipe en virtud de los trámites de apostilla o legalización no desconocieron los criterios formulados por la Corte en aquella oportunidad, por las razones que a continuación pasan a explicarse.

5.2. En efecto, tal como se advirtió en la SU-458 de 2012 lo que resultaba violatorio del derecho al hábeas data en dicho contexto era que la administración de los antecedentes judiciales de los ciudadanos no estuviera sometida a una precisa finalidad constitucional o legal, privilegiando un efecto perverso de favorecer el ejercicio inorgánico del poder informático al radicarlo en cabeza de cualquier persona con acceso a la base de datos cuestionada. Justamente, era aquella facilidad de la que podía valerse cualquier tercero sin ningún interés legítimo la que no podía encontrar asidero constitucional, puesto que “cualquier particular” podía conocer el pasado judicial de un individuo.

5.3. En el caso que ahora analiza la Sala sin embargo, la hipótesis no puede ser la misma. De acuerdo con los antecedentes expuestos, Felipe afirma que las accionadas vulneraron sus derechos al hábeas data y a la igualdad, al considerar que, aún tratándose de la expedición de un certificado de antecedentes judiciales con fines migratorios, debía aplicarse la misma solución adoptada en la SU-458 de 2012.

5.4. La Sala considera que si bien deben aplicarse los criterios allí puntualizados, no por ello debe llegarse a la misma solución. Esto, como quiera que la facultad de supresión relativa del titular de los datos personales, desarrollada por la sentencia de unificación, opera de la mano con los principios que orientan la administración de los mismos, particularmente con el principio de finalidad. Con relación a este último y de acuerdo con el numeral 3.5.2.3. de esta providencia,

para que el tratamiento y la divulgación de los datos se justifiquen constitucionalmente, el suministro de los mismos debe realizarse bajo un propósito (i) legítimo jurídicamente; (ii) exclusivo y (iii) específico.

5.4.1. Sobre el particular, la Sala encuentra que, en primer lugar, la solicitud del certificado de antecedentes judiciales por un Gobierno extranjero para la autorización de migrar hacia su territorio obedece a un propósito legítimo en el marco del bloque de constitucionalidad. Esto, en consideración a lo dispuesto por el artículo 3° de la Convención de Viena sobre Relaciones Diplomáticas de 1961,[81] puesto que dentro de las funciones de las misiones diplomáticas se encuentran, entre otras, la de “b) proteger en el Estado receptor los intereses del Estado acreditante y los de sus nacionales, dentro de los límites permitidos por el derecho internacional”, situación que se asemeja a la de las Oficinas Consulares, [82] en razón a lo previsto por el artículo 5° de la Convención de Viena sobre Relaciones Consulares de 1963.[83] En tal sentido, es apenas comprensible que los Estados, en virtud de su soberanía y otras políticas internas como pueden ser el control demográfico o poblacional así como las relacionadas con la seguridad o la política criminal, tomen medidas y establezcan requisitos para admitir a ciudadanos extranjeros en su territorio con fines migratorios, esto es, con el propósito de generar un posible establecimiento allí mediante el otorgamiento de visas, residencia o nacionalidades, tal como lo explicaba la Cancillería en su respuesta. Asimismo, esta situación no constituye una circunstancia desconocida en términos locales, dado que el Gobierno de Colombia, de conformidad con el Decreto 2268 de 1995, tal como en otros países, tiene competencia discrecional para autorizar el ingreso de extranjeros[84] e igualmente solicitar el certificado de antecedentes judiciales.

Por esta misma razón, es que las autoridades migratorias del posible país receptor sí son terceros con un interés legítimo de conocer el registro de los antecedentes judiciales de un ciudadano sin lugar a supresiones relativas, en este caso los del accionante, puesto que la restricción para acceder a la historia judicial de un ciudadano fue establecida por la Corte en la sentencia de unificación cuando se trataba de un tercero que, sin ningún interés legítimo o claramente definido en el ordenamiento, aspiraba a conocer los antecedentes delictivos de otra persona, situación que en el presente caso, por lo explicado no ocurre.

5.4.2. Frente a los asuntos de exclusividad y especificidad, en principio parecería que el móvil y el destino de la expedición de un certificado de antecedentes judiciales en el marco de todo lo que puede implicar un trámite consular podría parecer vago. Sin embargo, considerando lo sostenido por la Cancillería en esta sede, frente a que no todos los trámites consulares son de la misma naturaleza y que además pueden estar clasificados según su propósito migratorio o no, la Sala observa que asegurar dichos presupuestos sí es posible y que, de hecho, la Cancillería ha garantizado su observancia con el sistema diferencial que emplea actualmente.

En la medida en que la base de datos sea diseñada únicamente para la expedición del (i) certificado de antecedentes judiciales;[86] (ii) en un trámite de apostilla o legalización;[87] con un fin (iii) exclusivamente migratorio; (iv) con destino a un país o gobierno extranjero que, a su vez, constituye la autoridad competente y (v) frente a la cual deben adelantarse una serie de trámites específicos y con un propósito identificable (visa, nacionalidad o residencia), esta Sala concluye que el tratamiento y divulgación de dichos datos se justifican constitucionalmente.

Esta serie de medidas que se proponen, reitera la Sala, es posible hallarlas a lo largo del trámite de apostilla o legalización de antecedentes judiciales que las personas adelantan en la plataforma destinada para ello por la Cancillería, puesto que se debe seleccionar el tipo de documento que se

va a apostillar o legalizar,[88] se pregunta si el ciudadano “¿Requiere y autoriza la consulta y expedición del CERTIFICADO DE ANTECEDENTES JUDICIALES con fines migratorios?”,[89] y solicita, de forma obligatoria, el suministro del nombre del país de destino del documento.

5.5. En lo que hace a los principios de necesidad y utilidad, la Sala encuentra que la información relativa a los antecedentes judiciales suministrada en el curso de un trámite consular (apostilla y legalización) con fines migratorios, debe ser la estrictamente necesaria para el cumplimiento de la finalidad de la base de datos que, en este caso, sería el interés de una autoridad extranjera en conocer la existencia o no de antecedentes judiciales para estudiar una solicitud con propósitos migratorios al país que representa. En efecto, se observa que el certificado del accionante expedido por la Cancillería y contentivo de la leyenda “No tiene asuntos pendientes con las autoridades judiciales”, en contraste con el que se le expidió a su cónyuge, puede tenerse como indicativo de que alguna vez la persona fue condenada penalmente pero que la autoridad judicial competente declaró la extinción de la condena o la prescripción de la pena, es decir, que el documento no contiene información que desborde lo estrictamente requerido por la embajada respectiva y lo solicitado por el demandante, puesto que el interés de los gobiernos extranjeros es conocer, en últimas, si el ciudadano solicitante fue condenado penalmente alguna vez y si además es requerido por alguna autoridad judicial al momento del trámite migratorio.

5.6. Frente al principio de utilidad, la Corte advierte que, en la medida en que los responsables de la base de datos sobre antecedentes judiciales con fines migratorios (Policía Nacional y Cancillería) han mantenido la utilidad de la misma en forma clara y determinable, es decir, para suministrar la información necesaria, por ministerio de su titular, a autoridades extranjeras sin dotarla de otro tipo de funciones ajenas a ello y para las que el accionante dio su consentimiento, este principio se ha respetado.

En el siguiente cuadro, aportado por la Cancillería, se sintetiza la forma como dicha entidad, en compañía de la Policía Nacional, ha estado administrando la base de datos de antecedentes judiciales en los trámites de apostilla y legalización con y sin fines migratorios. A juicio de la Sala, además del procedimiento ya descrito, el contenido de los certificados de antecedentes judiciales en este contexto también ha observado los principios que informan la administración de bases de datos personales, particularmente el de necesidad y finalidad:

5.8. Con fundamento en lo expuesto, es que la Sala no considera que el derecho al hábeas data del peticionario fuera desconocido a la luz de la SU-458 de 2012, si además se suma a ello que en la misma providencia, este Tribunal inclusive reconoce que el “(...) control migratorio adelantado por autoridades de otros Estados (...), [tiene] un ámbito restringido y una finalidad más o menos precisa (...)”, así como que los usos de los antecedentes judiciales, “(...) en materia de inteligencia, ejecución de la ley y control migratorio” son plenamente legítimos.

Sin embargo, esta conclusión no implica que la solución del caso se limite al análisis exclusivo en relación con lo dicho en la sentencia de unificación. Como se propuso en las consideraciones generales, a juicio de la Sala resultaría pertinente, por las mismas particularidades del caso concreto, que su estudio se completara bajo las reglas que orientan el tema de la transferencia internacional de datos personales, que, a su vez, se encuentra estrechamente ligado con los principios de libertad, acceso y circulación restringida.

5.9. En efecto, la Sala no advierte violación alguna al principio de exigencia de estándares de protección equivalentes para la transferencia internacional de datos, puesto que tal y como están

diseñados los procedimientos migratorios ante las Embajadas o las oficinas consulares, estos, como representantes de otros Gobiernos, no son quienes solicitan la información directamente, obviando el consentimiento y la libertad informática que le asiste al titular de los datos, sino que es éste último y en este caso el señor Felipe, quien los solicita personalmente y consciente de que otros, con intereses legítimos como ya se explicó, los puedan conocer.

En ese sentido, el caso analizado puede ubicarse en la hipótesis de la excepción establecida por el literal a) del artículo 26 de la Ley Estatutaria 1581 de 2012, clara manifestación del principio de libertad en materia de administración de datos personales. En efecto, tal como se vio, esta excepción privilegia la autorización expresa e inequívoca del titular para una transferencia que, inclusive, él mismo se encuentra haciendo, puesto que en los trámites ante autoridades consulares extranjeras cuando se solicita una visa por ejemplo, tal como sucede en el caso concreto, son las personas interesadas quienes deben aportar los documentos correspondientes a su solicitud migratoria, lo que en efecto descarta cualquier modo de obviar su voluntad en la transferencia de los datos.

5.10. Finalmente, en tal sistema, donde es el titular quien adelanta todos los trámites sin ningún intermediario, también se garantiza el principio de acceso y circulación restringida, como quiera que al momento de acceder a la plataforma en línea ofrecida por la Cancillería para adelantar el trámite de apostilla o legalización de los antecedentes judiciales con fines migratorios, se solicitan una serie de datos con el propósito de asegurar que el solicitante del certificado sea el titular de los datos a consultar: (i) número de pasaporte y fecha de expedición del mismo, cuando se tiene pasaporte de lectura mecánica; (ii) último trámite realizado a través del Sistema Integrado de Trámites al Ciudadano –SITAC-, y fecha de realización del mismo y (iii) a falta de alguno de los anteriores, el sistema exige primero el registro, en el cual se deben indicar todos los datos personales y de localización del ciudadano. Adicionalmente, para la expedición exitosa del certificado debe cancelarse una tasa.

5.11. Por otra parte, el accionante alega que su derecho a la igualdad fue vulnerado, puesto que la diferenciación en el contenido de los certificados judiciales lo ubicaba en una posición de desigualdad y de desventaja frente a las personas que nunca habían cometido un delito. Sin embargo, a juicio de la Sala tampoco existe tal vulneración, como quiera que la diferenciación en el contenido del certificado de antecedentes judiciales entre las personas que han cometido delitos, habiéndose extinguido su condena o prescrito la pena, y las que nunca lo han hecho, ha sido reconocida por la jurisprudencia de esta Corporación como aceptable constitucionalmente siempre que, como ya se dijo, el acceso a tal información no ocurra en forma indiscriminada y su divulgación obedezca a los principios de finalidad, exclusividad, especificidad, necesidad, utilidad y libertad. En ese sentido, considerando que el otorgamiento de la información del pasado judicial del señor Felipe a un país extranjero bajo su consentimiento, se ajustó a los anteriores principios, los cuales justifican constitucionalmente la diferenciación de las leyendas en los certificados judiciales de él y su esposa-ésta última quien nunca ha cometido delitos-, la Sala advierte que no se configura una violación del derecho a la igualdad, puesto que a situaciones disímiles se ha otorgado un tratamiento distinto respaldado constitucionalmente.

5.12. Por lo visto, esta Sala considera que la sentencia del Consejo de Estado que decidió en segunda instancia la acción de tutela que ahora se revisa y amparó los derechos a la igualdad y al hábeas data debe ser revocada, por las razones desarrolladas en esta providencia y, en su lugar, debe negarse el amparo solicitado y procederse a la confirmación parcial, en tanto, dicha Corporación desestimó la petición especial relacionada con la protección de la identidad del

accionante, la cual se adoptó en la presente sentencia con el propósito de proteger los derechos contemplados en el artículo 15 constitucional y en consideración a que la presunta vulneración alegada por el actor tiene su génesis en relación con los mismos.

5.13. Finalmente, en virtud del impacto al proceso migratorio que con la decisión del Consejo de Estado se generó a los trámites consulares con dichos fines, esta Sala considera que la decisión adoptada debe cobijar no solamente el caso del accionante sino a toda la plataforma de apostilla o legalización de antecedentes judiciales para fines migratorios administrada por la Cancillería y la Policía Nacional.

III. DECISIÓN:

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

RESUELVE:

Primero.- REVOCAR la sentencia del 31 de julio de 2014, proferida por el Consejo de Estado-Sala de lo Contencioso Administrativo-Sección Cuarta, dentro del expediente T-4.516.485, y en su lugar, **CONFIRMAR PARCIALMENTE** la sentencia del 20 de mayo del mismo año, del Tribunal Administrativo de Cundinamarca- Sección 3, Subsección A-, mediante la cual se negó el amparo del derecho al habeas data y a la igualdad del señor Felipe, en los términos y por los motivos expuestos en esta providencia.

Segundo.- PREVENIR a la Cancillería y a la Policía Nacional para que conserven los parámetros sobre los cuales han edificado la plataforma de apostilla o legalización de antecedentes judiciales para fines migratorios de acuerdo con lo expuesto en el capítulo 5 de esta providencia, y adicionalmente, lo continúen aplicando no solo al caso del señor Felipe sino frente a todo el sistema relativo a la apostilla o legalización de antecedentes judiciales para fines migratorios, en virtud de lo expuesto en el numeral 5.12. de esta providencia.

Tercero.- **ORDENAR** que, por Secretaría General, se libren las comunicaciones a que se refiere el artículo 36 del Decreto 2591 de 1991.

Notifíquese, comuníquese, publíquese en la Gaceta de la Corte Constitucional y cúmplase.

LUIS GUILLERMO GUERRERO PÉREZ

Magistrado

GABRIEL EDUARDO MENDOZA MARTELO

Magistrado

GLORIA STELLA ORTIZ DELGADO

Magistrada

ANDRÉS MUTIS VANEGAS

Secretario General (E)

[1] Con el propósito de proteger los derechos contemplados en el artículo 15 constitucional y en consideración a que la presunta vulneración alegada por el actor tiene su génesis en relación con los mismos, la Sala omitirá de esta providencia y de toda futura publicación de la misma los nombres reales del accionante y de los demás miembros de su familia. En consecuencia, el demandante será llamado Felipe y su esposa Marina.

[2] El expediente de la referencia fue seleccionado para revisión por la Sala de Selección de Tutelas Número Diez, mediante auto del 06 de octubre de 2014. Folios 8 al 11 del cuaderno de revisión.

[3] "La apostilla es la legalización de la firma de un funcionario público en ejercicio de sus funciones cuya firma deberá estar registrada en la base de datos del Ministerio de Relaciones Exteriores. Se apostilla la firma del funcionario público impuesta en el documento mas no se certifica ni revisa su contenido. Un documento se debe apostillar cuando el país en el cual surtirá efectos es parte de la Convención sobre la Abolición del Requisito de Legalización para Documentos Públicos Extranjeros de la Haya de 1961. La apostilla también podrá imponerse sobre documento privado. La firma del documento privado deberá ser reconocida por notario público, la firma de éste último deberá estar registrada en la base de datos del Ministerio de Relaciones Exteriores.// La legalización consiste en reconocer la firma de funcionario público en ejercicio de sus funciones previo registro en la base de datos del Ministerio de Relaciones Exteriores para que el documento sea válido en otro país. Se legaliza la firma del funcionario público impuesta en el documento, más no se certifica ni revisa su contenido. Un documento se debe legalizar cuando el país en el cual surtirá efectos no hace parte de la Convención sobre la Abolición del Requisito de Legalización para Documentos Públicos Extranjeros de la Haya de 1961. La legalización también podrá imponerse sobre documento privado. La firma del documento privado deberá ser reconocida por notario público, la firma de éste último deberá estar registrada en la base de datos del Ministerio de Relaciones Exteriores."
http://www.cancilleria.gov.co/tramites_servicios/apostilla_legalizacion. Consultado el 7 de febrero de 2015.

[4] Oficio enviado por el Juzgado 11 de Ejecución de Penas y Medidas de Seguridad de Bogotá al Departamento Administrativo de Seguridad- DAS-, el 6 de agosto de 2008. Folio 26 del cuaderno principal.

[5] Ibídem.

[6] La actualización de información que reposa en la base de datos de la Dirección de Investigación Criminal e Interpol (DIJIN) fue confirmada al accionante el 18 de febrero de 2014, en respuesta a un derecho de petición por él presentado el 14 del mismo mes. Folio 21 del cuaderno principal.

[7] Respuesta del peticionario al cuestionario enviado en sede de revisión. Folio 19 del cuaderno de revisión.

[8] <https://antecedentes.policia.gov.co:7005/WebJudicial/formAntecedentes.xhtml>. Consultado el 10 de febrero de 2015.
<https://antecedentes.policia.gov.co:7005/WebJudicial/formAntecedentes.xhtml>. Consultado el 10 de febrero de 2015.

[9] Según dichos certificados, lo documentado allí "(...) solamente es válido para ser presentado ante la autoridades extranjeras toda vez que la información contenida en el portal web

www.policia.gov.co se ajusta a los parámetros establecidos en el ordenamiento constitucional colombiano". Folios 22 al 25 del cuaderno principal.

[10] La impugnación fue presentada el 30 de mayo de 2014. Folio 99 a 104 del cuaderno principal.

[11] "**PRIMERO.- ORDENAR** que, por Secretaría General, se inste al señor Felipe para que, en un término de 3 días hábiles a partir de la notificación de este auto, informe a este despacho (i) si el trámite para el cual requiere la apostilla/legalización de los antecedentes judiciales tiene fines migratorios; (ii) ¿para qué trámite (visa, pasaporte, nacionalidad) requiere la apostilla/legalización de sus antecedentes judiciales? y; (iii) ante qué país está adelantando dicho trámite.// **SEGUNDO.- ORDENAR** que, por Secretaría General, se oficie a la Cancillería- Ministerio de Relaciones Exteriores- para que, en un término de 3 días hábiles a partir de la notificación de este auto, responda el siguiente cuestionario, **señalando y adjuntando la normatividad que soporta cada una de las respuestas:** //

¿Qué se entiende por una solicitud con fines migratorios y otra con fines no migratorios?

¿Existe alguna diferencia en el contenido del certificado de antecedentes judiciales apostillado/legalizado, entre una solicitud con fines migratorios y otra sin esa finalidad?

Si la anterior respuesta es afirmativa, ¿Cuál es esa diferencia y a qué obedece la misma?

¿Existe alguna diferencia en el contenido del certificado de antecedentes judiciales apostillado/legalizado en función del país destinatario?

Si la anterior respuesta es afirmativa, ¿Cuál es esa diferencia, a qué obedece la misma y cómo se clasifican las exigencias que hace cada país frente a los antecedentes judiciales? (indicar los países)

Actualmente, ¿la Cancillería puede brindar información a países extranjeros sobre los antecedentes judiciales de un ciudadano colombiano por solicitud de aquellos?

Para tramitar la apostilla/legalización de antecedentes judiciales, ¿Qué datos deben proporcionarse?, y ¿Cómo se garantiza la autenticidad de que el titular es quien adelanta el mismo?

¿En qué forma están dando cumplimiento a la sentencia SU-458 de 2012 y bajo qué criterios?

¿Qué dificultades se han presentado con motivo del cumplimiento de la anterior sentencia para los trámites de apostilla/legalización de antecedentes judiciales?

¿Para otorgar algunos tipos de visados, Colombia exige el certificado de antecedentes judiciales o algún documento con contenido equivalente? Si la respuesta es afirmativa, ¿Qué tipo de especificidades exige el gobierno colombiano frente al certificado de antecedentes judiciales de dichos ciudadanos? ¿Alguna leyenda en especial?" Folios 14 y 15 del cuaderno de revisión.

[12] "El certificado deberá ser expedido por la autoridad competente del país de origen o último lugar de residencia donde haya permanecido el solicitante de la visa, mínimo 3 años; el mismo deberá estar debidamente apostillado o legalizado y traducido, según el caso. Si la permanencia ha sido en Colombia, bastara reporte que expide la Policía Nacional." Folio 22 del cuaderno de

revisión.

[13] Cuyos nombres, aunque mencionados por la Cancillería, no resulta pertinente publicar en esta providencia.

[14] "Tal como lo señala el profesor Mario G. Losano precursor muy fecundo tanto de la informática jurídica como del derecho informático en Italia, y cuyas obras son ampliamente conocidas en nuestro continente, un banco de datos no es otra cosa que un conjunto de informaciones que se refieren a un sector particular del conocimiento, las cuales pueden articularse en varias bases de datos y ser distribuídas a los usuarios de una entidad que se ocupa de su constante actualización y ampliación. //O lo que es fundamentalmente lo mismo, un conjunto de informaciones exhaustivas y no redundantes sobre un determinado tema, manejado por un específico conjunto de programas." Cfr. T-414 de 1992 (M.P. Ciro Angarita Barón) citando a Losano Mario G., Informatica per le scienze sociali Giulio Einaudi editore s.p.a., Torino 1985, pág. 315 y 316.

[15] Expresión utilizada por la sentencia T-307 de 1999 (M.P. Eduardo Cifuentes Muñoz).

[16] En la sentencia T-414 de 1992 (M.P. Ciro Angarita Barón), la Corte, siguiendo al profesor Vittorio Frosini, definió el poder informático.

[17] Sentencia T- 414 de 1992 (M.P. Ciro Angarita Barón).

[18] Sobre este aspecto, en la sentencia T-414 de 1992 (M.P. Ciro Angarita Barón) se señaló: "De estas inquietudes muy fundadas se han hecho también eco algunos instrumentos elaborados por organismos internacionales. Así, por ejemplo, en la denominada "Proclama de Teherán", aprobada por la Conferencia Internacional de Derechos Humanos el 13 de Mayo de 1968 se declaró solemnemente que: **"Si bien los recientes descubrimientos científicos y adelantos tecnológicos han abierto amplias perspectivas para el progreso económico, social y cultural, esta evaluación puede, sin embargo, comprometer los derechos y las libertades de los individuos y por ello requerirá una atención permanente"**. // También en su "Declaración sobre la utilización del progreso científico y tecnológico en interés de la paz y en beneficio de la humanidad", proclamada por la Asamblea General de las Naciones Unidas el 10 de noviembre de 1975 se expresa que: **"Todos los Estados tomarán medidas apropiadas a fin de impedir que los progresos científicos y tecnológicos sean utilizados, particularmente por órganos estatales, para limitar o dificultar el goce de los derechos humanos y las libertades fundamentales de la persona consagrados en la Declaración Universal de Derechos Humanos, en los Pactos Internacionales de Derechos Humanos y en otros instrumentos internacionales pertinentes"**. (Subrayado original)

[19] De acuerdo con la Sentencia C-1011 de 2008 (M.P. Jaime Córdoba Triviño), debe tenerse en cuenta que la denominación "hábeas data" no ha sido la única utilizada por la jurisprudencia para identificar las facultades del sujeto concernido respecto de las bases de datos. Así, durante el desarrollo del concepto en las decisiones de la Corte se han usado las expresiones de "autodeterminación informática" o "autodeterminación informativa". En todo caso, estas tres definiciones refieren a la misma realidad jurídica, por lo que no ofrecen mayores dificultades en su uso alternativo.

[20] Esta equivalencia se pone de manifiesto en la sentencia SU- 082 de 1995 (M.P. Jorge Arango Mejía) en la cual la Corte afirma que el derecho a la autodeterminación informática, constituye el "núcleo esencial" del derecho al habeas data. En el mismo sentido Cfr., sentencias

T-552 de 1997 (M.P. Vladimiro Naranjo Mesa) y T-307 de 1999 (M.P. Eduardo Cifuentes Muñoz).

[21] El primer desarrollo del derecho al hábeas data y sus relaciones con los derechos a la dignidad humana, la intimidad y el buen nombre fue realizado por la Corte en la sentencia T-414 de 1992 (M.P. Ciro Angarita Barón). En esta sentencia se consideró que la protección del dato personal era un aspecto connatural a la eficacia del derecho a la intimidad, en cuanto es el individuo quien debe arbitrar la divulgación de la información perteneciente a su vida privada.

Este ejercicio del derecho constitucional adquiría, en términos de la sentencia, una mayor vigencia ante las posibilidades de gestión informatizada de datos que ejercían las centrales de información financiera. De esa medida, existía la necesidad de configurar a favor del individuo un derecho a la "libertad informática", definido como "la facultad de disponer de la información, de preservar la propia identidad informática, es decir, de permitir, controlar o rectificar los datos concernientes a la personalidad del titular de los mismos y que, como tales, lo identifican e individualizan ante los demás. Es, como se ve, una nueva dimensión social de la libertad individual diversa, y por razón de las circunstancias que explican su aparición, de otras clásicas manifestaciones de la libertad".

[22] En las sentencias T-094 de 1995 (M.P. José Gregorio Hernández Galindo), T-097 de 1995 (M.P. José Gregorio Hernández Galindo), y T-119 de 1995 (M.P. José Gregorio Hernández Galindo), la Corte, a pesar de reconocer al habeas data como "derecho autónomo", sigue tratándolo como garantía, en la medida en que lo considera un instrumento para la protección de otros derechos como la intimidad, la honra y el buen nombre.

[23] Cfr. Sentencia T- 307 de 1999 (M.P. Eduardo Cifuentes Muñoz).

[24] El fundamento de validez de los llamados principios de la administración de datos personales, se encuentra en el segundo inciso del artículo 15 de la Constitución, el cual constituye en términos de la Corte, "el contexto normativo y axiológico dentro del cual debe moverse, integralmente el proceso informático" y del cual derivan "unas reglas generales que deben ser respetadas para poder afirmar que el proceso de acopio, uso y difusión de datos personales sea constitucionalmente legítimo", y que a su vez son el resultado "de la aplicación directa de las normas constitucionales al proceso informático." Así, en sentencia T-307 de 1999 (M.P. Eduardo Cifuentes Muñoz).

[25] En efecto, para una adecuada comprensión de la colisión entre los derechos a la información y al habeas data, la Corte propone una tipología de la información que, mediante el manejo de criterios más o menos estables, facilite la unificación de la jurisprudencia constitucional y la seguridad jurídica entre los actores más usuales de los mismos. La primera gran tipología, es aquella dirigida a distinguir entre la información impersonal y la información personal. En función de la especialidad del régimen aplicable al derecho a la autodeterminación, esta diferenciación es útil principalmente por tres razones: la primera, es la que permite afirmar que en el caso de la información impersonal no existe un límite constitucional fuerte al derecho a la información, sobre todo teniendo en cuenta la expresa prohibición constitucional de la censura (artículo 20 inciso 2º), sumada en algunos casos a los principios de publicidad, transparencia y eficiencia en lo relativo al funcionamiento de la administración pública (artículo 209) o de la administración de justicia (artículo 228). Una segunda razón, está asociada con la reconocida diferencia entre los derechos a la intimidad, al buen nombre y al habeas data, lo cual implica reconocer igualmente las diferencias entre su relación con la llamada información personal y su posible colisión con el derecho a la información. La tercera razón, guarda relación con el régimen

jurídico aplicable a los llamados procesos de administración de datos inspirado por principios especiales y en el cual opera, con sus particularidades, el derecho al habeas data.

[26] Sentencia T-414 de 1992 (M.P. Ciro Angarita Barón).

[27] Cfr. Corte Constitucional, sentencia T-729 de 2002 (M.P. Eduardo Montealegre Lynett), fundamento jurídico 4 c).

[28] Cfr. T-729 de 2002 (M.P. Eduardo Montealegre Lynett).

[29] En la sentencia T-307 de 1999 (M.P. Eduardo Cifuentes Muñoz), sobre la llamada información "sensible", la Corte afirmó: "(...)no puede recolectarse información sobre datos "sensibles" como, por ejemplo, la orientación sexual de las personas, su filiación política o su credo religioso, cuando ello, directa o indirectamente, pueda conducir a una política de discriminación o marginación."

[30] De conformidad con la sentencia C-1011 de 2008 (M.P. Jaime Córdoba Triviño): "Estos datos no son susceptibles de acceso por parte de terceros, salvo que se trate en una situación excepcional, en la que el dato reservado constituya un elemento probatorio pertinente y conducente dentro de una investigación penal y que, a su vez, esté directamente relacionado con el objeto de la investigación. En este escenario, habida cuenta la naturaleza del dato incorporado en el proceso, la información deberá estar sometida a la reserva propia del proceso penal."

[31] En dicha oportunidad, la Corte resolvió el caso de la circulación de datos personales de contenido crediticio sin el consentimiento del titular de los datos. Es así como la Corte, bajo la necesidad de "favorecer una plena autodeterminación de la persona" y ante la "omisión de obtener la autorización expresa y escrita del titular para la circulación de sus datos económicos personales", resolvió conceder la tutela de los derechos a la intimidad y al debido proceso y ordenó a la central de información financiera el bloqueo de los datos personales del actor.

[32] Véase esta cualificación del consentimiento como libre, previo y expreso, en sentencia SU-082 de 1995 (M.P. Jorge Arango Mejía).

[33] En la misma sentencia de unificación se afirmó que: "los datos conseguidos, por ejemplo, por medios ilícitos no pueden hacer parte de los bancos de datos y tampoco pueden circular." En forma similar, en la Sentencia T-176 de 1995 (M.P. Eduardo Cifuentes Muñoz), se consideró como una de las hipótesis de la vulneración del derecho al habeas data el de la recolección de información "de manera ilegal, sin el consentimiento del titular de dato."

[34] Cfr. sentencia T-729 de 2002 (M.P. Eduardo Montealegre Lynett).

[35] Ibídem.

[36] "La recopilación y el registro de información personal en computadoras, bancos de datos y otros dispositivos, tanto por las autoridades públicas como por las particulares o entidades privadas, deben estar reglamentados por la ley. Los Estados deben adoptar medidas eficaces para velar por que la información relativa a la vida privada de una persona no caiga en manos de personas no autorizadas por ley para recibirla, elaborarla y emplearla y porque nunca se la utilice para fines incompatibles con el Pacto. Para que la protección de la vida privada sea lo más eficaz posible, toda persona debe tener el derecho de verificar si hay datos personales suyos almacenados en archivos automáticos de datos y, en caso afirmativo, de obtener información

inteligible sobre cuáles son esos datos y con qué fin se han almacenado. Asimismo, toda persona debe poder verificar qué autoridades públicas o qué particulares u organismos privados controlan o pueden controlar esos archivos. Si esos archivos contienen datos personales incorrectos o se han compilado o elaborado en contravención de las disposiciones legales, toda persona debe tener derecho a pedir su rectificación o eliminación". Cfr. Comité de Derechos Humanos.

Observación General No. 16 "El Derecho al respecto a la vida privada, la familia, el domicilio, y la correspondencia y la protección de la honra y la reputación". Adoptada durante el 32º período de sesiones. 1988. Párrafo 10.

[37] En el ámbito del sistema interamericano, el Relator para la Libertad de Expresión expuso consideraciones más amplias sobre el alcance del derecho del titular de acceso a la información personal. Al respecto, el principio 3º de la Declaración de Principios sobre Libertad de Expresión, establece que "Toda persona tiene el derecho a acceder a la información sobre sí misma o sus bienes en forma expedita y no onerosa, ya esté contenida en bases de datos, registros públicos o privados y, en el caso de que fuere necesario, actualizarla, rectificarla y/o enmendarla". Al analizar este principio, el Relator indicó lo siguiente:

"Este principio se refiere a la acción de habeas data. La acción de habeas data se erige sobre la base de tres premisas: 1) el derecho de cada persona a no ser perturbado en su privacidad, 2) el derecho de toda persona a acceder a información sobre sí misma en bases de datos públicos y privados para modificar, anular o rectificar información sobre su persona por tratarse de datos sensibles, falsos, tendenciosos o discriminatorios y 3) el derecho de las personas a utilizar la acción de habeas data como mecanismo de fiscalización. Este derecho de acceso y control de datos personales constituye un derecho fundamental en muchos ámbitos de la vida, pues la falta de mecanismos judiciales que permitan la rectificación, actualización o anulación de datos afectaría directamente el derecho a la privacidad, el honor, a la identidad personal, a la propiedad y la fiscalización sobre la recopilación de datos obtenidos.// Esta acción adquiere una importancia aún mayor con el avance de nuevas tecnologías. Con la expansión en el uso de la computación e Internet, tanto el Estado como el sector privado tienen a su disposición en forma rápida una gran cantidad de información sobre las personas. Por lo tanto, es necesario garantizar la existencia de canales concretos de acceso rápido a la información para modificar información incorrecta o desactualizada contenida en las bases de datos electrónicas. Asimismo la acción de habeas data impone ciertas obligaciones a las entidades que procesan información: el usar los datos para los objetivos específicos y explícitos establecidos; y garantizar la seguridad de los datos contra el acceso accidental, no autorizado o la manipulación. En los casos en que antes del Estado o del sector privado hubieran obtenido datos en forma irregular y/o ilegalmente, el peticionario debe tener acceso a dicha información, inclusive cuando ésta sea de carácter clasificada.// En cuanto al carácter fiscalizador de la acción de habeas data, es importante destacar que en algunos países del hemisferio, dicha acción constituye un importante mecanismo de control de la actividad de las agencias de seguridad e inteligencia del Estado. El acceso a los datos personales permite verificar la legalidad utilizada por parte de estas agencias del Estado en la recopilación de datos de las personas. El acceso a dicha información, por otra parte, habilita al peticionario a conocer la identidad de los involucrados en la recopilación ilegal de datos, habilitando la sanción legal para sus responsables. // Para que la acción de habeas data sea llevada a cabo con eficiencia, se deben eliminar las trabas administrativas que obstaculizan la obtención de la información y deben implementarse sistemas de solicitud de información de fácil acceso, simples y de bajo costo para el solicitante. De lo contrario, se consagraría formalmente una acción que en la práctica no contribuye a facilitar el acceso a la información.

Asimismo, es necesario que para el ejercicio de dicha acción, no se requiera revelar las causas por las cuales se requiere la información. La mera existencia de datos personales en registros públicos o privados es razón suficiente para el ejercicio de este derecho". Cfr. Relatoría para la Libertad de Expresión. Informe Anual CIDH, 2000, volumen 3. Página 1. Párrafos 12-15.

[38] Finalmente, en el ámbito interamericano, la Organización de los Estados Americanos, OEA, encargó al Comité Jurídico Interamericano elaborar varios informes sobre el acceso y protección de la información y los datos personales. En noviembre de 2010, se expide el "Proyecto de principios y recomendaciones preliminares sobre la protección de datos". El trabajo realizado por el Comité Jurídico Interamericano señaló que existen dos sistemas de protección de bases de datos "el europeo es hoy el sistema más estricto de regulaciones estatales, con una legislación que rige la recolección de datos personales por el gobierno y las entidades privadas. El sistema de Estados Unidos sigue un criterio bifurcado, que permite que los sectores económicos regulen los datos personales recabados por el Estado. Por último, varios países de América Latina han elaborado mecanismos de protección de datos basados en el concepto de habeas data, que permite a las personas acceder a sus propios datos personales y otorga el derecho".

[39] El artículo 5 del mismo convenio advierte que los datos deben: "ser obtenidos legalmente y tratados de la misma forma; ser registrados para finalidades específicas y lícitas, por lo que no podrán ser utilizados con distintos fines; ser adecuados, pertinentes y acordes con las finalidades para las cuales fueron previstas, ser exactos y puestos al día; ser conservados de tal forma que permita la identificación de las personas que fueron concernidas durante un periodo de tiempo que no exceda del necesario para el cual fue registrado." Éste último literal guarda relación con lo que podría llamarse el principio de temporalidad, entendido éste como aquél que ordena que el dato no podrá ser utilizado más allá del tiempo para el que fue previsto, y por lo tanto, la consecuencia natural de ello, es su exclusión de la base de datos dentro de la cual fue registrado, con el fin de evitar que la información allí consignada pueda ser usada para fines distintos, como aquellos con propósitos ilícitos o fraudulentos o de carácter comercial.

[40] La Resolución 45/95 de la ONU, "principios rectores sobre la reglamentación de ficheros computarizados de datos personales" desarrolla los siguientes: // Principio de la licitud y lealtad. Está dirigido concretamente a que la información de las personas no sea recolectada en forma ilícita ni utilizarse para fines contrarios a los propósitos y principios de la Carta de las Naciones Unidas.// Principio de exactitud. Pretende que las personas encargadas del tratamiento deben verificar la exactitud y certeza de los datos, procurando la actualización periódica de los mismos.// Principio de finalidad: La finalidad para la cual es utilizada la información contenida en ficheros, debe ser específica y clara. Igualmente, debe comunicársele al titular de la información sobre su utilización, para que pueda asegurarse que:// "Todos los datos personales reunidos y registrados siguen siendo pertinentes a la finalidad perseguida"; Ninguno de esos datos personales es utilizado o revelado sin el consentimiento de la persona interesada, con un propósito incompatible con el que se haya especificado; El periodo de conservación de los datos personales no excede del necesario para alcanzar la necesidad con que se han registrado."// Principio de acceso a la persona interesada. Permite al usuario, una vez identificado, conocer si la información que se relaciona con su información personal está siendo utilizada y a obtener las correcciones necesarias cuando la información es inexacta y a que se le informe si los datos han sido transmitidos a terceros. En este sentido, el propio mandato señala una posibilidad para que en cada ordenamiento se cree una herramienta jurídica que le permita al usuario ejercer un recurso. Señala expresamente la Resolución: "Debería preverse una vía de recurso, en su caso, ante la autoridad encargada del control de conformidad con el principio 8 infra. En caso de

rectificación, el costo debería rectificarlo el responsable del fichero [quien trata la información]. Es conveniente que las disposiciones de este principio se apliquen a todas las personas, cualquiera que sea su nacionalidad o su residencia"// Principio de no discriminación. Prohíbe el registro de datos que puedan generar en la persona algún tipo de discriminación, en particular sobre el origen racial o étnico, color, vida sexual, opiniones políticas, convicciones religiosas, filosóficas o de otro tipo, o sobre la participación en una asociación o la afiliación a un sindicato.// Facultad de establecer excepciones: Permite establecer excepciones respecto de los principios 1 a 4, cuando se trate de: i) proteger la seguridad nacional, ii) el orden público, iii) la salud o la moral pública y iv)"en particular, los derechos y libertades de los demás, especialmente de personas perseguidas (cláusula humanitaria), a reserva de que estas excepciones se hayan previsto expresamente por la ley o por una reglamentación equivalente, adoptada de conformidad con el sistema jurídico nacional, en que se definan expresamente los límites y se establezcan las garantías apropiadas". Principio de seguridad: Se deberán adoptar medidas necesarias para proteger los ficheros contra riesgos naturales, como la pérdida accidental o la destrucción por siniestro, y contra los riesgos humanos, como el acceso sin autorización, la utilización encubierta de datos o la contaminación por virus informático.// Principio relativo a los controles y sanciones: "Cada legislación debería designar a la autoridad que, de conformidad con el sistema jurídico interno, se encarga de controlar el respeto de los principios anteriormente enunciados". Conforme este postulado, la autoridad debe ofrecer garantía de imparcialidad, independencia respecto de organismos o personas responsables del procesamiento de datos y su aplicación. Igualmente, señala que debería preverse sanciones penales o de otro tipo, cuando se violen las disposiciones de cada legislación.// Principio sobre el flujo de datos a través de las fronteras. El flujo de información entre dos países o más, puede darse siempre y cuando sus legislaciones sean comparables respecto de la garantía de protección de la vida privada, para que la información pueda correr libremente como en el país de origen. Finalmente dispone que "cuando no haya garantías comparables, no se podrán obtener limitaciones injustificadas a dicha circulación, y solo en la medida que así lo exija la protección de la vida privada".

[41] Por su parte, la Directiva 95/46/CE, sistematiza las directrices del manejo de los datos y reconoce que tales disposiciones se encuentran encaminadas a "la protección de las libertades y de los derechos fundamentales a las personas físicas y, en particular, del derecho a la intimidad, en lo que respecta al tratamiento de datos personales" (artículo 1). El instrumento divide los principios en dos categorías: (i) los relativos a la calidad del dato y (ii) los concernientes a la legitimidad en el manejo de la información.// En relación con los primeros dispone (artículo 6) que los datos personales sean: "(i) Tratados de manera leal y lícita, (ii) Recogidos con fines determinados, explícitos y legítimos, y no sean tratados posteriormente de manera incompatible con dichos fines; no se considerará incompatible el tratamiento posterior de datos con fines históricos, estadísticos o científicos, siempre y cuando los Estados miembros establezcan las garantías oportunas, (iii) Adecuados, pertinentes y no excesivos con relación a los fines para los que se recaben y para los que se traten posteriormente, (iv) Exactos y, cuando sea necesario, actualizados; deberán tomarse las medidas razonables para que los datos inexactos o incompletos, con respecto a los fines para los que fueron recogidos o para los que fueron tratados posteriormente, sean suprimidos o rectificadas, (v) Conservados en una forma que permita la identificación de los interesados durante un periodo no superior al necesario para los fines para los que fueron recogidos o para los que se traten ulteriormente. Los Estados miembros establecerán las garantías apropiadas para los datos personales archivados por un periodo más largo al mencionado, con fines históricos, estadísticos o científicos."// En cuanto a los segundos, la Directiva establece que el manejo de los datos sólo puede realizarse con el consentimiento

inequívoco del titular y cuando es necesario : (i) "para la ejecución de un contrato en el que el interesado sea parte o para la aplicación de medidas precontractuales.", (ii) "para el cumplimiento de una obligación jurídica a la que esté sujeto el responsable del tratamiento", (iii) "para proteger el interés vital del interesado", (iv) para el cumplimiento de una misión de interés público o inherente al ejercicio del poder público conferido al responsable del tratamiento o a un tercero a quien se comuniquen los datos" y (v) para la satisfacción del interés legítimo perseguido por el responsable del tratamiento o por el tercero o terceros a los que se comuniquen los datos siempre que no prevalezca el interés o los derechos y libertades fundamentales del interesado que requieran protección con arreglo al apartado 1 de la presente directiva".

[42] La legitimidad está relacionada con la licitud en el procesamiento de datos y la justicia, se refiere a que en el procesamiento de los mismos no se puede dar lugar factores de discriminación contra una persona. Estas nociones, están consignadas en la "Resolución de Madrid", un documento producto de la "Propuesta Conjunta para la Redacción de Estándares Internacionales para la protección de la Privacidad, en relación con el Tratamiento de Datos de carácter personal", acogido favorablemente por la 31 Conferencia Internacional de Autoridades de Protección de Datos y Privacidad, celebrada el 5 de noviembre de 2009 en Madrid, España.

[43] El límite al procesamiento de datos significa que este debe ser adecuado, relevante y no excesivo frente a los propósitos para los cuales se recabaron. La necesidad indica que debe hacerse lo posible para limitar el procesamiento de datos a lo estrictamente necesario.

[44] Está referido a que el controlador de datos debe ofrecer a la persona la información suficiente para que esta tenga la opción de establecer una relación de transparencia con aquel.

[45] Sostiene que el controlador de datos es responsable de adoptar todas las medidas necesarias para seguir las pautas del procesamiento de datos personales que imponga la legislación nacional u otra autoridad competente.

[46] que a su vez contiene las reglas para que se considere válido el procesamiento de datos, esto es que exista "a) consentimiento, b) interés legítimo del controlador, c) las obligaciones contractuales, d) una autoridad legal y e) circunstancias excepcionales, como cuando la información es necesaria para atenuar o evitar un perjuicio irremediable."

[47] En virtud del cual el controlador puede usar tales sistemas siempre que asegure el nivel de protección y que el nivel de protección sea establecido por una relación contractual.

[48] Señala que las transferencias internacionales de datos sólo deberán efectuarse si el país receptor, ofrece, como mínimo, el mismo nivel de protección de datos personales que brindas los principios aquí reseñados.

Adicionalmente, este principio desarrolla los factores para determinar si un país receptor otorga las normas mínimas de protección de datos: 1) la naturaleza de los datos; 2) el país de origen; 3) el país receptor; 4) el propósito para el cual se procesan los datos, y 5) las medidas de seguridad vigentes para la transferencia y el procesamiento de datos personales.

[49] El derecho de acceso el derecho de la persona solicitar y obtener del controlador de datos información sobre sus datos personales.

[50] La persona tiene derecho a solicitar que el controlador de datos corrija o suprima los datos personales que puedan ser incompletos, inexactos, innecesarios o excesivos.

[51] La persona podría objetar el procesamiento de sus datos personales en los casos en que exista una razón legítima, como perjuicio o angustia injustificada y sustancial para ella.

[52] Establece que el controlador de datos y el procesador de datos deben disponer de medidas técnicas y de organización razonables para garantizar la integridad, confidencialidad y disponibilidad de los datos personales.

[53] Los controladores de datos y los procesadores de datos tienen el deber de mantener la confidencialidad de todos los datos personales, inclusive más allá de terminada la relación entre la personal y el controlador de datos.

[54] Con el fin de asegurar el cumplimiento y la aplicación de los principios de la protección de datos, la OEA señala que debe disponerse de una autoridad supervisora y establecerse un recurso judicial para las personas. Sobre la autoridad, señala que esta debe ser imparcial e independiente. Asimismo, debe contar con capacidad técnica, facultades y recursos suficientes para realizar investigaciones y auditorías a fin de asegurar el cumplimiento de las normas pertinentes.

[55] "En primer lugar, cabe señalar que el proyecto acoge una clasificación especial de principios que no incluye la totalidad de los principios predicables de la administración de datos y que han sido desarrollados tanto por la jurisprudencia de esta Corporación, como por las normas internacionales sobre la materia. Sin embargo, tal y como se consideró en la Sentencia C-1011 de 2008, al estudiar la constitucionalidad de los principios predicables a la administración de datos del sistema financiero y crediticio, las previsiones que integran el artículo 4 deben interpretarse de forma tal que resulten compatibles con la Carta Política. En consecuencia, si la Corte - intérprete autorizado de la Constitución-, ha definido a través de los principios de administración de datos personales el contenido y alcance del derecho fundamental al hábeas data, las normas estatutarias deberán interpretarse en armonía con el plexo de garantías y prerrogativas que integran ese derecho. Además, también serán analizados a la luz de los estándares internacionales sobre la materia."

[56] "El régimen de protección de datos personales que se establece en la presente ley no será de aplicación:// a) A las bases de datos o archivos mantenidos en un ámbito exclusivamente personal o doméstico. Cuando estas bases de datos o archivos vayan a ser suministrados a terceros se deberá, de manera previa, informar al Titular y solicitar su autorización. En este caso los Responsables y Encargados de las bases de datos y archivos quedarán sujetos a las disposiciones contenidas en la presente ley; b) A las bases de datos y archivos que tengan por finalidad la seguridad y defensa nacional, así como la prevención, detección, monitoreo y control del lavado de activos y el financiamiento del terrorismo; c) A las Bases de datos que tengan como fin y contengan información de inteligencia y contrainteligencia; d) A las bases de datos y archivos de información periodística y otros contenidos editoriales; e) A las bases de datos y archivos regulados por la Ley 1266 de 2008; f) A las bases de datos y archivos regulados por la Ley 79 de 1993."

[57] Adicionalmente, esta conclusión también fue sostenida por la SU-458 de 2012 (M.P. Adriana María Guillén Arango): "Es jurisprudencia constante de esta Corte en materia de habeas data, que la administración de toda base de datos personales está sometida a los llamados principios de administración de datos personales. Recientemente, el Legislador aprobó una serie de principios contenidos en el proyecto de ley estatutaria general de habeas data, proyecto que en este punto fue declarado ajustado a la Constitución mediante sentencia C-748 de 2011. Asimismo, la Corte en sentencia C-1011 de 2008, consideró que los principios contenidos en la

ley estatutaria de habeas data financiero eran constitucionales y que, además, su aplicación era extensiva a todas las bases de datos personales sin importar que la regulación estudiada tenía un marcado carácter sectorial."

[58] Cfr. C-536 de 2006 (M.P. Humberto Antonio Sierra Porto) y C-243 de 2005 (M.P. Álvaro Tafur Galvis). En esta última providencia, se examinó la exequibilidad de los artículos primero de la Ley 15 de 1968 y 10 de la Ley 4 de 1981, disposiciones que autorizaban al Gobierno Nacional a reglamentar lo relacionado con los modelos y el valor de las cédulas de extranjería, certificados judiciales y otros documentos expedidos por el Departamento Administrativo de Seguridad.

[59] El extinto Departamento Administrativo de Seguridad DAS fue creado mediante el Decreto 1717 de 1960, en sustitución del llamado Servicio de Inteligencia Colombiano -SIC-, a su vez creado por el Decreto 2872 de 1953.

[60] Mediante la cual se creó el Fondo Rotatorio del Departamento Administrativo de Seguridad.

[61] "Decreto 218 de 2000. ARTÍCULO 3º.- Funciones. El Departamento Administrativo de Seguridad tendrá, además de las funciones que determina el artículo 59 de la Ley 489 de 1998, las siguientes: 13º. Llevar los registros delictivos y de identificación nacionales, y expedir los certificados judiciales, con base en el canje interno y en los informes o avisos que deben rendir oportunamente las autoridades judiciales de la República."

☐ [62] Decreto 0233 de 2012 del Ministerio de Defensa Nacional. "Artículo 2. La Dirección de Investigación Criminal e INTERPOL tendrá, además de las funciones señaladas en los Decretos 4222 de 2006 y 216 de 2000, y en disposiciones legales especiales, las siguientes: 1. Organizar, actualizar y conservar los registros delictivos nacionales, de acuerdo con los informes, reportes o avisos que para el efecto deberán remitirle las autoridades judiciales competentes, conforme a la Constitución Política y a la ley, sobre iniciación, tramitación y terminación de procesos penales, órdenes de captura, medidas de aseguramiento, autos de detención, enjuiciamiento, revocatorias proferidas y sobre las demás determinaciones previstas en el Código de Procedimiento Penal. // 2. Implementar y gestionar los mecanismos de consulta en línea que permitan el acceso a la información sobre los antecedentes judiciales que reposen en los registros delictivos, de acuerdo con los protocolos que se adopten para el efecto. // 3. Garantizar que la información contenida en las bases de datos mantengan los niveles de seguridad requeridos, de acuerdo a su naturaleza. // 4. Garantizar el acceso y consulta a la información que reposa en los registros delictivos a la Fiscalía General de la Nación, autoridades que ejerzan funciones de policía judicial, autoridades judiciales y administrativas que en razón de sus funciones y competencias lo requieran, de conformidad con sus competencias constitucionales y legales. // 5. Las demás que se requieran para la implementación y gestión del registro delictivo."

[63] Sentencia T-542 de 2003 (M.P. Marco Gerardo Monroy Cabra)

[64] Cfr. SU-458 de 2012 (M.P. Adriana María Guillén Arango). En dicha oportunidad, también se mencionó que, en la sentencia T-023 de 1993, la Corte, empleando fuentes secundarias, tomó la siguiente definición de la expresión antecedentes penales: "los hechos y circunstancias relativos a una persona, anteriores a un momento dado, constituyen sus antecedentes. Referidos a la totalidad de la vida, representan su biografía; así es frecuente hablar de sus antecedentes sanitarios, morales, profesionales, familiares, etc. Sus antecedentes penales estarán circunscritos a los castigos que hayan sido judicialmente impuestos a ese individuo como sanción de delitos o

infracciones por él cometidos".

[65] Cfr. Sentencia C-185 de 2003 (M.P. Eduardo Montealegre Lynett).

[66] Cfr. Sentencia SU-458 de 2012 (M.P. Adriana María Guillén Arango).



[67] Según el numeral 1° del artículo 55 del Código Penal (en adelante CP) la carencia de antecedentes penales es circunstancia de menor punibilidad. El artículo 68 A del CP prohíbe la concesión de cualquier subrogado penal a quien haya sido condenado por delito doloso o preterintencional dentro de los cinco (5) años anteriores. Según el inciso 2° del artículo 1° de la Ley 750 de 2002, para que los padres cabeza de familia puedan cumplir la pena privativa de la libertad en su lugar de residencia, deben, entre otros, no registrar antecedentes penales, etc. Igualmente, en materia penitenciaria y carcelaria, por ejemplo, según los artículos 147 y 147 A de la Ley 65 de 1993, "no ser requerido por autoridad judicial" (clásica fórmula de certificación de los antecedentes penales) es indispensable para la procedencia de los permisos de salida (por 72 horas y hasta por 15 días) a los reclusos que cumplan además otros requisitos.

[68] Por ejemplo, de acuerdo con los artículos 179 numeral 1°, y 197 de la Constitución, no puede ser congresista ni presidente de la República quien haya sido condenado "en cualquier época, por sentencia judicial, a pena privativa de la libertad, excepto por delitos políticos o culposos". Igualmente, de conformidad con el artículo 122, inciso 5 (modificado mediante artículo 1° del AL 1 de 2004, y artículo 4° del AL de 2009) de la Constitución, no podrán ser inscritos como candidatos, ni elegidos, ni designados como servidores públicos, ni contratar con el Estado, "quienes hayan sido condenados, en cualquier tiempo, por la comisión de delitos que afecten el patrimonio del Estado o quienes hayan sido condenados por delitos relacionados con la pertenencia, promoción o financiación de grupos armados ilegales, delitos de lesa humanidad o por narcotráfico en Colombia o en el exterior."

[69] En materia de inteligencia y contrainteligencia, la información relacionada con antecedentes penales, al decir del entonces DAS, "es relevante (...) puesto que coadyuva a establecer el grado de peligrosidad de una persona y su historial criminal". Esto de conformidad con los numerales 1, 3, 5 y 7, del artículo 2° del Decreto 643 de 2004, todos relacionados con las actividades de inteligencia y contrainteligencia del entonces DAS o de quien en la actualidad haya asumido tales funciones.



[70] Artículos 33 y 34 del Decreto Ley 2535 de 1993.



[71] Ley 43 de 1993, artículo 25 parágrafo 2.



[72] Artículo 105 literal g del Decreto 2737 de 1989, Código del Menor.

[73] De acuerdo con la SU-458 de 2012 (M.P. Adriana María Guillén Arango): "[L]a obligación constitucional de crear un banco de datos donde conste la existencia de hechos delictivos atribuibles a una persona, [desvirtúa que su] permanencia y publicación [en forma de antecedentes penales], después de decretada la extinción o la prescripción de la pena, equivalga a una pena perpetua violatoria de la prohibición constitucional de penas imprescriptibles (art. 18 Superior)".

[74] "Artículo 26. Prohibición. Se prohíbe la transferencia de datos personales de cualquier tipo a países que no proporcionen niveles adecuados de protección de datos. Se entiende que un país ofrece un nivel adecuado de protección de datos cuando cumpla con los estándares fijados por la Superintendencia de Industria y Comercio sobre la materia, los cuales en ningún caso podrán ser inferiores a los que la presente ley exige a sus destinatarios.// Esta prohibición no regirá cuando se trate de:// a) Información respecto de la cual el Titular haya otorgado su autorización expresa e inequívoca para la transferencia; b) Intercambio de datos de carácter médico, cuando así lo exija el Tratamiento del Titular por razones de salud o higiene pública; c) Transferencias bancarias o bursátiles, conforme a la legislación que les resulte aplicable; d) Transferencias acordadas en el marco de tratados internacionales en los cuales la República de Colombia sea parte, con fundamento en el principio de reciprocidad; e) Transferencias necesarias para la ejecución de un contrato entre el Titular y el Responsable del Tratamiento, o para la ejecución de medidas precontractuales siempre y cuando se cuente con la autorización del Titular; f) Transferencias legalmente exigidas para la salvaguardia del interés público, o para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial. // Parágrafo 1°. En los casos no contemplados como excepción en el presente artículo, corresponderá a la Superintendencia de Industria y Comercio, proferir la declaración de conformidad relativa a la transferencia internacional de datos personales. Para el efecto, el Superintendente queda facultado para requerir información y adelantar las diligencias tendientes a establecer el cumplimiento de los presupuestos que requiere la viabilidad de la operación.// Parágrafo 2°. Las disposiciones contenidas en el presente artículo serán aplicables para todos los datos personales, incluyendo aquellos contemplados en la Ley 1266 de 2008."

[75] Cfr. Sentencia C-748 de 2011 (M.P. Jorge Ignacio Pretelt Chaljub).

[76] Cfr. Sentencia C-748 de 2011 (M.P. Jorge Ignacio Pretelt Chaljub).

[77] REMOLINA ANGARITA, Nelson. Tratamiento de datos personales. Aproximación internacional y comentarios a la Ley 1581 de 2012. LEGIS, Bogotá, 2013, Págs. 250 a 251.



[78] El Grupo de Trabajo fue creado por el artículo 29 de la Directiva 95/46/CE. Es un órgano consultivo independiente de la UE sobre protección de datos y vida privada. Sus funciones son definidas en el artículo 30 de la citada Directiva y en el artículo 14 de la Directiva 97/66/CE.

[79] Cfr. Sentencia C- 748 de 2011 (M.P. Jorge Ignacio Pretelt Chaljub).

[80] Ibídem.

[81] La Convención de Viena sobre Relaciones Diplomáticas de 1961 fue introducida en el ordenamiento jurídico interno colombiano a través de la Ley 60 de 1972.

[82] La Convención de Viena sobre Relaciones Consulares de 1963 fue introducida en el ordenamiento jurídico colombiano a través de la Ley 17 de 1971.



[83] "ARTÍCULO 5. Las funciones consulares consistirán en: a) proteger en el Estado receptor los intereses del Estado que envía y de sus nacionales, sean personas naturales o jurídicas, dentro de los límites permitidos por el derecho internacional."

[84] "ARTÍCULO 1o. Es competencia discrecional del Gobierno Nacional autorizar el ingreso de

extranjeros al país. // Corresponde al Ministerio de Relaciones Exteriores expedir, negar o cancelar visas.// El ingreso de extranjeros, así como su permanencia o salida del territorio nacional se regirán por las disposiciones de este Decreto y las políticas del Gobierno Nacional, sin perjuicio de lo dispuesto en los tratados internacionales y de conformidad con la competencia discrecional antes mencionada."

[85] "ARTÍCULO 32. La visa de residente podrá ser otorgada por la División de Visas del Ministerio de Relaciones Exteriores o por los agentes consulares autorizados por la Cancillería.

El solicitante de dicha visa, salvo el refugiado y el asilado, deberá presentar, sin perjuicio de lo que se exige en cada categoría, los siguientes documentos:// 1. Pasaporte vigente o documento de viaje.// 2. Prueba del estado civil o parentesco, si fuere el caso.// 3. Certificado de antecedentes judiciales o de policía del último país de domicilio, expedido por autoridad competente con una antelación no mayor de seis (6) meses. Se exceptúa de este requisito a los menores de 18 años y a los mayores de 60 años de edad.// 4. Certificado médico expedido con una antelación no mayor de seis (6) meses, por un médico registrado en el Consulado de Colombia o ante la autoridad competente, en el que conste que el solicitante, no padece de enfermedad infectocontagiosa ni mental."

[86] Puesto que existen otros documentos que también son susceptibles de apostilla o legalización, como el Certificado de Antecedentes Disciplinarios, el Certificado de venta libre INVIMA, la Notificación sanitaria obligatoria INVIMA, el Pasaporte con Zona de Lectura Mecánica, entre muchos otros.

http://www.cancilleria.gov.co/tramites_servicios/apostilla_legalizacion. Consultado el 10 de febrero de 2015.

[87] Esta precisión, en tanto, existen otros trámites y servicios consulares además de la apostilla y legalización, como la expedición de pasaportes, visas, los trámites de nacionalidad y cooperación Judicial; así como los trámites que pueden adelantarse en el exterior, relacionados con el Registro civil, la Tarjeta de identidad, la Cédula de ciudadanía, las Certificaciones / Constancias, la Autenticación de documentos, el Reconocimiento de firma en documento privado, el Reconocimiento de firma en autorización de salida del menor o la Protocolización de escrituras públicas. http://www.cancilleria.gov.co/tramites_servicios/tramites_exterior. Consultado el 10 de febrero de 2015.

[88] <https://tramites.cancilleria.gov.co/apostillalegalizacion/solicitudtramite/inicio.aspx>. Consultado el 6 de febrero de 2015.

[89] <https://tramites.cancilleria.gov.co/Ciudadano/certificadoAntecedentes/solicitud.aspx>. Consultado el 6 de febrero de 2015.



Última actualización: 31 de diciembre de 2019

