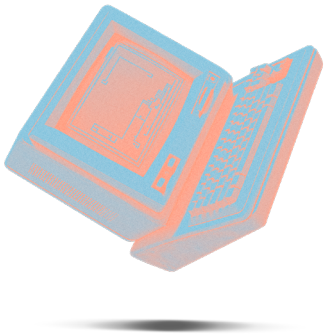
EL VEINTE

¿UNIDAD DE DESPROTECCIÓN DE DATOS?:

diagnóstico del mecanismo gubernamental de protección en clave de privacidad y seguridad digital



Redacción:
Susana Echavarría Medina
Pablo Ceballos Navas

Investigación:
Susana Echavarría Medina
Pablo Ceballos Navas
Lucía Yepes Bonilla

Edición:
Ana Bejarano Ricaurte
Emmanuel Vargas Penagos

Diseño y diagramación:
Sergio Solarte

El Veinte, 2023.

EL VEINTE

INTRODUCCIÓN

La violencia contra la prensa en Colombia es un fenómeno en aumento. En 2022, la Fundación para la Libertad de Prensa (FLIP) registró 218 amenazas contra periodistas, la cifra más alta en los últimos 15 años y el homicidio de dos periodistas. En los últimos 3 años cinco periodistas han sido asesinados por razones relacionadas a su trabajo[1]. Reporteros Sin Fronteras señala que Colombia es uno de los países más peligrosos para ejercer el periodismo; la prensa se encuentra permanentemente expuesta a intimidaciones, acoso y violencia[2]. Ante las precarias condiciones de seguridad para la prensa, y en seguimiento de la obligación estatal de "prevenir, proteger y procurar justicia"[3], el Estado debe prever medidas para la definición y adopción de mecanismos de protección específicos que atiendan los riesgos identificados y garanticen la integridad y seguridad de los periodistas en riesgo.

En respuesta a los actos de violencia contra periodistas, el gobierno nacional, por medio del Decreto 1592 de 2000, creó el "Programa de Protección a Periodistas y Comunicadores Sociales" a cargo de la dirección general para los derechos humanos del Ministerio de Interior para aquellos periodistas que, en ejercicio de su profesión, se encontraran en situación de riesgo o amenaza contra su vida, integridad, seguridad o libertad[4]. Más adelante, en reemplazo del anterior mecanismo, el Decreto 4065 de 2011 creó la Unidad Nacional de Protección (UNP).

1. Fundación para la Libertad de Prensa (FLIP), "Páginas para la libertad de expresión", Quinta Edición, 2023, https://flip.org.co/publicaciones/informes/quinta-edicion-paginas
2. Reporteros sin frontera, "Clasificación: Puntuación Global", 2023, https://rsf.org/es/clasificacion
3. Comisión Interamericana de Derechos Humanos, Relatoría Especial para la Libertad de Expresión, "Violencia contra periodistas y trabajadores de medios: Estándares interamericanos y prácticas nacionales sobre prevención, protección y procuración de la justicias", 2013, https://www.oas.org/es/cidh/expresion/docs/informes/2014_04_22_Violencia_ESP_WEB.pdf
4. Decreto 1592 de 2000, artículo 1

La UNP es la entidad encargada de prestar y garantizar la oportunidad, eficiencia e idoneidad del servicio de protección a quienes, en virtud de sus actividades, condiciones o situaciones vitales, se encuentren en un riesgo extraordinario o extremo contra su integridad, libertad o seguridad personal o colectiva[5]. El modelo de protección vigente, en razón del riesgo determinado en cada caso particular, podrá asignar esquema de protección -compuesto por vehículo, conductor(es) y escolta(s)- con los recursos físicos requeridos, medios de movilización, apoyo para reubicación temporal, apoyo para trasteo, equipos de comunicación, blindaje de inmuebles e instalación de sistemas técnicos de seguridad y botón de pánico[6].

La sola protección física, en todo caso, no garantiza la efectividad de la medida. El Estado debe además implementar una política integral que garantice la protección de los beneficiarios, en particular de los periodistas en riesgo, desde múltiples dimensiones. Según se establece en la Sentencia Bedoya Lima y otra v. Colombia de la Corte Interamericana de Derechos Humanos (CorteIDH), las medidas de protección deben asegurar que "los y las periodistas que laboran en los medios de comunicación gocen de la protección y de la independencia necesarias para realizar sus funciones a cabalidad"[7]. Lo anterior se sostiene, además, en lo dicho por la misma Corte en la Sentencia Defensor de derechos humanos y otros v. Guatemala en la que se estableció que el programa de protección adoptado por el Estado debe "abordar de forma integral e interinstitucional la problemática de acuerdo con el riesgo de cada situación"[8]. De esta manera, como también ha sido reconocido por la Corte Constitucional, las medidas deben superar la protección de la seguridad e integridad física y deben atender, contextualmente, la complejidad del riesgo. Específicamente, en la Sentencia T-1037 de 2008 la Corte Constitucional estableció que "la persona amenazada no sólo tiene derecho a la seguridad. Adicionalmente tiene derecho a las menores restricciones colaterales posibles como efecto de las medidas de protección adoptadas"[9].

La preponderancia de la garantía de la privacidad de solicitantes y beneficiarios es, en gran medida, parte integral de la protección misma. Por esta razón, la UNP no debe desatender la estrecha relación entre la observancia de la privacidad y el cumplimiento de su mandato de protección. De allí, que la Corte Constitucional, en la Sentencia T-294 de 2023, exhorte a la UNP a través de su director a adoptar las medidas necesarias para el cumplimiento de la Política de Tratamiento y Protección de Datos Personales de la entidad que, según el fallo, debe alinearse con la regulación de protección de datos personales, regida principalmente por la Ley Estatutaria 1581 de 2012. Bajo esta perspectiva, cobra sentido un análisis específico sobre el mecanismo de protección en clave de protección de la privacidad y seguridad digital.

Para la adjudicación de los respectivos mecanismos de protección, salvo cuando se

5. A diferencia del "Programa de Protección a Periodistas y Comunicadores Sociales" las medidas de protección de la UNP no son exclusivas para periodistas y comunicadores sociales. Los Decretos 1066 de 2015 y 1487 de 2018 enlistan las 16 poblaciones que son objeto del Programa de Protección de la UNP.
6. Decreto 1066 de 2015, artículo 2.4.1.2.11
7. Corte Interamericana de Derechos Humanos, Bedoya Lima y otra v. Colombia, Sentencia de 26 de agosto de 2021. Serie C No. 431, párr. 152.
8. Corte Interamericana de Derechos Humanos, Defensor de derechos humanos v. Guatemala, Sentencia de 28 de agosto de 2014. Serie C No. 283, párr. 263
9. Corte Constitucional, Sentencia T-1037 de 2008, M.P. Jaime Córdoba Triviño.

trate de medidas de emergencia asignadas en casos de riesgo inminente y excepcional, se requiere de la valoración integral del riesgo por parte del Comité de Evaluación de Riesgo y Recomendación de Medidas (CERREM) para una posterior recomendación de las medidas de protección y complementarias que resulten adecuadas al caso concreto. Este procedimiento, así como la solicitud de protección, el análisis de pertinencia de la solicitud y la evaluación de riesgo realizada por el Cuerpo Técnico de Análisis de Riesgo (CTAR), exigen de un exhaustivo análisis del solicitante, traduciéndose entonces en un volumen considerable de información personal, incluso sensible, recolectada en cada caso. En el caso de los periodistas y teniendo en cuenta que dicha información, que puede poner de presente los riesgos para el solicitante, podrían estar estrechamente relacionados con el ejercicio de su labor -para efectos de esta investigación, periodística-, su alcance y naturaleza puede resultar altamente delicado y amenazar aspectos trascendentales y especialmente protegidos de su profesión.

Posteriormente, tras la adopción de la medida de protección y durante su implementación, seguimiento y evaluación, la Unidad Nacional de Protección recopila datos personales de los beneficiarios, que están, además, directamente relacionados con la ejecución de la medida de protección, por ejemplo, la ubicación y movimientos de los protegidos en los vehículos de la UNP. **Esta cuestión que, como se observará a continuación, ha sido asumida como un trámite corriente en el desarrollo de las funciones de la entidad, repercute contundentemente en la privacidad, integridad, libertad y seguridad de los solicitantes, posteriores beneficiarios, y tiene efectos en el cumplimiento mismo de la protección.**

Este diagnóstico del mecanismo gubernamental de protección en clave de privacidad y seguridad digital, si bien aterriza un análisis que comprende la totalidad de las medidas de protección en relación con el tratamiento de datos personales y su concordancia con el marco regulatorio de privacidad, se enfoca principalmente en las experiencias y estándares aplicables para la protección de periodistas. Para este fin se realizó una revisión detallada de la normativa y jurisprudencia constitucional sobre habeas data, privacidad y protección de periodistas en riesgo. Asimismo, se analizó la política interna de privacidad y tratamiento de datos personales de la UNP, los formularios y lineamientos con la información requerida para la solicitud de una medida de protección y la clase de información recolectada en la adopción y evaluación de las diferentes medidas de protección, clasificación solicitada directamente a la entidad. Finalmente, para contrastar el marco normativo con experiencias de beneficiarios, se entrevistó a periodistas que han recibido medidas de protección por parte de la UNP, así como a la Fundación para la Libertad de Prensa desde su experiencia en la asesoría en protección de periodistas en riesgo.

El diagnóstico comprende, en primer lugar, un mapeo del marco legal aplicable en clave de privacidad y tratamiento de datos personales en las funciones de la Unidad Nacional de Protección; en segundo lugar, un análisis de los lineamientos en vigencia que rigen la solicitud de protección, la evaluación del riesgo, la recomendación de las medidas de protección y complementarias adecuadas, así como su implementación, seguimiento y evaluación en clave de privacidad y seguridad digital; en tercer lugar, contrastará las experiencias de beneficiarios y expertos con las disposiciones legales sobre protección de datos personales en materia de recolección de información de solicitantes y beneficiarios de sistemas de protección de la UNP; finalmente, una serie de conclusiones y recomendaciones.

MARCO REGULATORIO DE LA PROTECCIÓN DE DATOS PERSONALES EN COLOMBIA A LA LUZ DE LA POLÍTICA DE PRIVACIDAD DE LA UNIDAD NACIONAL DE PROTECCIÓN

El derecho fundamental al habeas data está consagrado en el artículo 15 de la Constitución Política. A su vez, y con el objetivo de desarrollar y regular su ejercicio, se promulgó la Ley 1518 de 2012, normativa de naturaleza estatutaria que circunscribió su ámbito de aplicación a los "datos personales registrados en cualquier base de datos"[10] que sean tratados o susceptibles de serlo por parte de personas naturales, jurídicas de derecho privado y entidades estatales. Acto seguido, el Legislador precisó de manera taxativa los casos que se exceptúan de la observancia de esta norma, entre los cuales se encuentra aquella información recolectada y organizada con propósitos de "seguridad y defensa nacional"[11] o "que tengan como fin y contengan información de inteligencia y contrainteligencia"[12]. En todo caso, la UNP no ejerce funciones de inteli-

10. Ley 1581 de 2012, artículo 2.
11. Ley 1581 de 2012, artículo 2, literal b).
12. Ley 1581 de 2012, artículo 2, literal c).

gencia ni hace parte de las fuerzas públicas[13] y, por ende, debe cumplir plenamente con la Ley de Habeas Data.

Otro punto relevante por considerar es la autorización del titular de la información para la recolección y almacenamiento de sus datos. Dispone la ley que la regla general es que el responsable del tratamiento de la información debe contar con consentimiento previo, expreso e informado del titular, por lo cual proscribe la obtención o procesamiento sin autorización. Como excepción a ese mandato, el Legislador dispuso unas causales taxativas, enlistadas en el artículo 10° de la precitada ley, entre ellas la "información requerida por una entidad pública o administrativa en ejercicio de sus funciones legales"[14]. Si bien esta disposición podría relevar a la entidad del requisito de contar con la autorización del titular de la información, no lo exime de la sujeción a la norma en cita -en particular de la aplicación completa e integral de los principios de legalidad, finalidad, libertad, veracidad, transparencia, acceso y circulación restringida, seguridad y confidencialidad en los términos del artículo 4° de la Ley 1581 de 2012-[15] ni le faculta para compartir con terceros los datos obtenidos con ocasión de sus funciones.

El Decreto 4065 de 2011, acto de constitución de la Unidad Nacional de Protección, señala como funciones de la institución, entre otras, las siguientes:

- "Implementar los programas de protección que determine el Gobierno Nacional, de competencia de la Unidad, dirigidos a salvaguardar los derechos a la vida, la libertad, la integridad y la seguridad personal".

- "Hacer seguimiento y evaluación a la oportunidad, idoneidad y eficacia de los programas y medidas de protección implementadas, así como al manejo que de las mismas hagan sus beneficiarios y proponer las mejoras a que haya lugar".

- "Realizar la evaluación del riesgo a las personas que soliciten protección, dentro del marco de los programas que determine el Gobierno Nacional, de competencia de la Unidad, en coordinación con los organismos o entidades competentes".

- "Administrar el sistema de información de protección".

Lo cierto es que existe entonces una consideración en la norma que debe atenderse en lineamiento con los principios internacionales e internos que regulan la materia. Por un lado, la mencionada Ley de Habeas Data no señala a la UNP como aquellas

13. La Unidad Nacional de Protección es una unidad administrativa especial adscrita al Ministerio de Interior y perteneciente al sector Interior, cuyas funciones están relacionadas en el artículo 4° del Decreto 4065 de 2011 y entre las cuales no se observa la atribución de competencias para actividades de inteligencia o contrainteligencia. Por otra parte, el artículo 216 constitucional dispone que "[l]a fuerza pública estará integrada en forma exclusiva por las Fuerzas Militares y la Policía Nacional" y seguidamente indica que constituyen las Fuerzas Militares "el Ejército, la Armada y la Fuerza Aérea".

14. Ley 1581 de 2012, artículo 10.

15. La misma Corte Constitucional –en sede de control previo al proyecto de ley que devendría en la Ley 1581 de 2012– sostuvo que aún si concurre una excepción a la aplicación de la Ley 1581 de 2012, deben observarse los principios contenidos en el artículo 4 de la referida norma por cuanto constituyen "garantías mínimas de protección del habeas data" (Sentencia C-748 de 2011, M.P. Jorge Ignacio Pretelt Chaljub).

entidades exentas de su cumplimiento, pero en menor medida sí señala que podrán recolectarse y almacenarse datos en cumplimiento de sus funciones legales. En todo caso, de optar por la interpretación según la cual la UNP sí puede adelantar esa tarea, esta potestad comporta múltiples limitaciones. La más estricta es la atinente a la información de menores de edad, que bajo ningún concepto podrá ser conservada por el responsable del tratamiento de datos. Una segunda restricción tiene que ver con el concepto del dato sensible, definido en el artículo 5° de la Ley 1581 y que comprende toda aquella información "que afect[e] la intimidad del titular o cuyo uso indebido puede generar su discriminación"[16]. Entre ellos, establece el mismo artículo, se encuentran aquellos datos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o partidistas; los datos sobre la salud y la vida sexual; así como los datos biométricos. Aunque el umbral de protección a este tipo de datos es elevado, también admite el tratamiento sin autorización del titular por parte de entidades estatales en ejercicio de sus funciones[17]. La información recaudada por la UNP podría incluir esta información y de hecho con certeza lo hace cuando se trata de periodistas o defensores de derechos humanos que realizan labores informativas que tratan estos temas o pertenecen a tales poblaciones históricamente discriminadas.

No existen pronunciamientos de la Corte Constitucional referentes al alcance de la expresión "intimidad" en el apartado citado. Sin embargo, la amplitud de la definición legal del dato sensible permite incluir en éste la información sobre el núcleo familiar, las relaciones afectivas y amistosas, la ubicación, las expresiones sobre asuntos contenciosos, el ejercicio del derecho a la reunión y, en el caso puntual de los periodistas, el contacto con fuentes de información, el trabajo investigativo y las conversaciones previas a la publicación, entre otros elementos propios del ejercicio del oficio. De igual manera, admiten ser tratados como datos sensibles los rasgos antropomórficos del individuo, la voz, la expresión y la apariencia.

En el curso de la solicitud, adopción y evaluación de medidas de protección, se recolectan múltiples datos de carácter sensible de los cuales es responsable por su tratamiento la Unidad Nacional de Protección. Por ejemplo, en los formularios que diligencian los solicitantes para la valoración de las solicitudes y de los esquemas concedidos se suelen recaudar, entre otros, (i.) los nombres, actividades y direcciones de residencia de los familiares del evaluado o protegido; (ii.) los antecedentes de amenazas en contra del evaluado o protegido; (iii.) la indicación sobre si algún integrante del núcleo familiar padece discapacidades; (iv.) la naturaleza de las relaciones afectivas del examinado; (v.) la relación de movimientos y la distinción de éstos según su propósito –habituales, por motivos personales o por trabajo–; (vi.) la indicación de las rutas que se siguen para los desplazamientos rutinarios; (viii.) la identificación del en-

16. Ley 1581 de 2012, artículo 5.
17. Ley 1581 de 2012, artículo 6, literal a); artículo 10, literal a).

torno social, laboral y residencial del examinado; y (ix.) la categorización de las rutas seleccionadas mediante un cuestionario que comprende preguntas sobre la hora de desplazamiento, la iluminación del camino, si el evaluado se moviliza solo o en compañía, entre otras[18].

Resulta altamente necesario la armonización entre dos elementos en tensión, pues la Unidad Nacional de Protección solicita, recolecta y gestiona información tan próxima a la esfera íntima de solicitantes y beneficiarios, cuando al mismo tiempo los principios rectores del programa de protección disponen que en su "planeación, ejecución, seguimiento y evaluación el Programa de Prevención y Protección tendrá en cuenta el conjunto de derechos constitucionales fundamentales de los que son titulares los protegidos, en el marco del principio de correlación entre deberes y derechos"[19]. Esto, en todo caso, debe conciliarse con estándares internacionales de privacidad y protección de datos personales que establecen, además de los principios contenidos en el artículo 4° de la Ley 1581 de 2012, el principio de proporcionalidad y el principio de minimización, ambos estrechamente relacionados con el principio de finalidad. El primero impone limitaciones al tratamiento de datos personales, es decir, siempre dirigido al cumplimiento de los fines para los cuales fueron recopilados los datos. El segundo determina que los datos recolectados deben ser los mínimos indispensables para la realización del objeto pretendido[20].

De vuelta a los principios rectores del habeas data, la Ley 1581 de 2012 establece la transparencia como principio y conmina a los encargados y responsables del tratamiento a poner en disposición del titular toda la información que de éste provenga, sin demora ni alteración, por cuanto es su derecho "conocer, actualizar y rectificar" los datos personales que posee el encargado o el responsable del tratamiento. Para ello, instituye un término de 10 días hábiles para su entrega, prorrogables por otros cinco días laborables si se presenta un retraso motivado[21]. Por su parte, el Decreto 1377 de 2013 confiere al titular el derecho a consultar "de forma gratuita sus datos personales [...] al menos una vez cada mes calendario".[22]

Incluso si se adoptara la tesis según la cual la UNP no debe pedir autorización de sus protegidos periodistas y similares para la recolección y almacenamiento de datos, no puede perderse de vista que la Ley 1581 de 2012 exige que el titular de la información sea informado de la finalidad que se persigue con el tratamiento de datos, obligación en la que el Legislador no distingue entre aquellos casos en los que el titular debe prestar su consentimiento y aquellos en los que no se requiere su anuencia.

De igual forma, el principio de finalidad demanda que en cualquier caso la finalidad

18. Esta información, sea para la solicitud del programa de prevención y protección individual o colectivo, se encuentra publicada en la página web de la UNP y fue proporcionada en respuesta al derecho de petición enviado para esta investigación (última fecha de consulta: 24 de octubre de 2023). Ruta individual: https://www.unp.gov.co/wp-content/uploads/2022/08/GSC-FT-11-V7-FORMULARIO-DE-SOLICITUD-DE-INSCRIPCIO%CC%81N-PARA-EL-PROGRAMA-DE-PREVENCIO%CC%80N-Y-PROTECCIO%CC%80N-QUE-COORDINA-LA-UNP-RUTA-INDIVIDUAL-1.pdf Ruta colectiva: https://www.unp.gov.co/wp-content/uploads/2022/08/gsc-ft-12-v5-FORMULARIO-DE-SOLICITUD-DE-INSCRIPCIO%CC%81N-PARA-EL-PROGRAMA-DE-PREVENCIO%CC%81N-Y-PROTECCIO%CC%81N-QUE-COORDINA-LA-UNP-RUTA-COLECTIVA-2.pdf
19. Decreto Único Reglamentario 1066 de 2015, artículo 2.4.1.2.2, numerales 5 y 10.
20. Naciones Unidas, Relatoría Especial sobre el derecho a la privacidad del Alto Comisionado para los Derechos Humanos, "Principios que informan la privacidad y la protección de datos personales", A/77/196, 2022, https://www.ohchr.org/es/documents/thematic-reports/a77196-principles-underpinning-privacy-and-protection-personal-data
21. Ley 1581 de 2012, artículo 14.
22. Decreto 1377 de 2013, artículo 21.

perseguida debe ser legítima, es decir, que no debe contravenir principios, derechos y garantías constitucionales. En sede de control previo de constitucionalidad, la Corte agregó que en suma de ser legítimo, el propósito del tratamiento de datos debe ser específico y explícito, quiere decir esto, "que la referida información se destinará a realizar los fines exclusivos para los cuales fue entregada por el titular".[23]

Si ocurre que la finalidad es ilegítima, el titular de la información –en hipótesis de tratamiento por parte de entidades estatales en ejercicio de sus competencias– puede solicitar la eliminación de la información recaudada, previo pronunciamiento de la autoridad nacional de datos personales que declare la comisión de la conducta reprochada y habiendo agotado la instancia de solicitud al responsable o al encargado del tratamiento.[24] Por ejemplo, en caso de enterarse que se registran y almacenan datos con el fin de perfilar o vigilar ilegalmente la actividad periodística, la finalidad en ese caso sería ilegítima y se habilitaría la posibilidad de eliminar la información recaudada.

La solicitud de supresión de información prevista en el artículo 9° del Decreto 1377 de 2013, establece que: "[l]a solicitud de supresión de la información [...] no procederán cuando el Titular tenga un deber legal o contractual de permanecer en la base de datos".[25] Por tanto deberá ponderarse y argumentarse qué representa mayor riesgo para el periodista, si la permanencia en la base de dato que ha sido señalado como ilegítima o mal utilizada o su retiro de la misma a pesar del acto administrativo que admite para revisión la solicitud de protección o del que la concede tras superar el examen de riesgo, la cual llamaría a que se registren sus datos a largo plazo en todo caso o hasta cesar la amenaza.

En suma de ser legítima, determinada y explícita, la finalidad debe orientar al responsable del tratamiento a recolectar aquellos datos que son pertinentes y adecuados. Bien lo asentó la Corte en su examen de constitucionalidad previa: "se encuentra prohibido el registro y divulgación de datos que no guarden estrecha relación con el objetivo de la base de datos. En consecuencia, debe hacerse todo lo razonablemente posible para limitar el procesamiento de datos personales al mínimo necesario".

Si existe sospecha de que la información recaudada no guarda consonancia con la finalidad perseguida o la excede, puede formularse una solicitud ante la Superintendencia de Industria y Comercio –autoridad nacional de datos personales– para que ordene al responsable entregar un reporte en el que describa "las finalidades para las cuales la información es recolectada" y explique "la necesidad de recolectar los datos en cada caso".[26]

23. Corte Constitucional, Sentencia C-748 de 2011, M.P. Jorge Ignacio Pretelt Chaljub.
24. Ley 1581 de 2012, artículo 16.
25. Decreto 1377 de 2013, artículo 9.
26. Decreto 1377 de 2013, artículo 4.

Además de los requisitos de legitimidad, explicitud, pertinencia, estrecha relación y necesidad, el Decreto 1377 de 2013 impone un mandato adicional que acota temporalmente el tratamiento de datos a un término "razonable y necesario, de acuerdo con las finalidades que justificaron el tratamiento, atendiendo a las disposiciones aplicables a la materia [...] y a los aspectos administrativos, contables, fiscales, jurídicos e históricos de la información"[27], pasado el cual deben suprimirse los datos personales con los que cuente el responsable o encargado. Sin perjuicio de lo anterior, la norma excluye de este mandato aquellos datos que se requieran "para el cumplimiento de una obligación legal o contractual"[28], lo cual deja la puerta abierta para que la Unidad Nacional de Protección pueda reclamar la vigencia del tratamiento de datos hasta tanto se dicte resolución que descarte la solicitud o que termine la medida de protección. Resulta problemático, como se ha venido mencionando, que dicha resolución dependa enteramente de la voluntad de la entidad, incluso cuando existan dudas o evidencia de su uso abusivo e ilegítimo de los datos recolectados.

Por otra parte, el precitado decreto prescribe una obligación adicional para el responsable del tratamiento cuando éste comprende datos sensibles. Dispone el numeral segundo del artículo sexto que deberá: "[i]nformar al titular de forma explícita y previa, además de los requisitos generales de la autorización para la recolección de cualquier tipo de dato personal, cuáles de los datos que serán objeto de Tratamiento son sensibles y la finalidad del Tratamiento, así como obtener su consentimiento expreso".[29] En el caso objeto de revisión, si bien respecto de la autorización opera la excepción por tratarse de información solicitada por una entidad pública en ejercicio de sus funciones, es admisible exigir la categorización de la información sensible así como la expresión de la finalidad perseguida con la recolección, en tanto y en cuanto la ley no hace distinción sobre este particular entre aquel dato sensible obtenido con autorización expresa y aquel que prescinde de ese requisito por la calidad pública del responsable. En otras palabras, incluso si se favorece la interpretación de que no se necesita autorización del titular, ello no exime a la entidad de la categorización y consecuente protección llamada para los datos sensibles.

Esta postura se robustece al examinar el derecho reconocido al titular y previsto en el literal c) del artículo 8° de la Ley 1581 de 2012, que se lee "[a] ser informado por el Responsable del Tratamiento o el Encargado del Tratamiento, previa solicitud, respecto del uso que le ha dado a sus datos personales"[30], así como al reparar en el deber específico atribuido al responsable del tratamiento y según el cual deberá "[i]nformar debidamente al Titular sobre la finalidad de la recolección y los derechos que le asisten por virtud de la autorización otorgada".[31]

27. Decreto 1377 de 2013, artículo 11.
28. Ibíd.
29. Decreto 1377 de 2013, artículo 6, numeral 2.
30. Ley 1581 de 2012, artículo 8.
31. Ley 1581 de 2012, artículo 17, literal c).

En relación con la vigilancia del cumplimiento de la Ley 1581 de 2012, el Legislador atribuyó la competencia jurisdiccional a la Delegatura para la protección de datos personales de la Superintendencia de Industria y Comercio y le asignó la función establecida en el literal c) del artículo 21° que otorga la disposición de "bloqueo temporal de los datos cuando, de la solicitud y de las pruebas aportadas por el Titular, se identifique un riesgo cierto de vulneración de sus derechos fundamentales, y dicho bloqueo sea necesario para protegerlos mientras se adopta una decisión definitiva".[32] Esta facultad, de naturaleza precautoria y cautelar, podría ser de gran valor para conocer la posición de la autoridad nacional de datos personales y, en el mejor de los casos, obtener un pronunciamiento favorable a la garantía de derechos humanos en el tratamiento de datos personales. Sobre este asunto se debe precisar que la norma defiere la competencia sancionatoria –es decir, la imposición de las multas previstas en el artículo 23° de la misma ley– a la Procuraduría General de la Nación cuando el responsable del tratamiento sea un funcionario público o una entidad estatal, pero no hace distinción en punto de las acciones jurisdiccionales y de las medidas cautelares.

EL PROCEDIMIENTO DE SOLICITUD, ADOPCIÓN Y EVALUACIÓN DE MEDIDAS DE PROTECCIÓN DE LA UNIDAD NACIONAL DE PROTECCIÓN EN CONCORDANCIA CON EL RÉGIMEN DE HABEAS DATA

Si bien la Unidad Nacional de Protección adoptó un Manual de políticas específicas de seguridad privacidad de la información que se rige, entre otras, por la ley 1581 de 2012 y el Decreto 1377 de 2013, en la aplicación, sea desde algunas previsiones mismas de los lineamientos internos o por los vacíos y testimonios de solicitantes y beneficiarios, se identifican claros vacíos y tensiones entre las prácticas de

32. Ley 1581 de 2012, artículo 21, literal c).

la UNP y la normativa vigente en materia de habeas data. A continuación un recuento de anotaciones y aclaraciones:

La Unidad Nacional de Protección (UNP) está sometida a la Ley 1581 de 2012

La entidad no califica para ninguna de las excepciones a la jurisdicción de la Ley de Habeas Data, en tanto pertenece al sector interior y ejerce funciones que no están previstas en la lista taxativa de exclusiones contenida en el artículo 2° de esa ley.

La Corte Constitucional en la Sentencia T-294 de 2023 observa que, según la "Política de Tratamiento y Protección de Datos Personales de la Unidad Nacional de Protección" adoptada en la Resolución 1848 del 26 de diciembre de 2018, la entidad reconoce expresamente "que administra datos personales en tanto requiere, para el ejercicio de sus funciones, recolectar información de los ciudadanos e incorporarla a una base de datos, al igual que dar tratamiento a esos datos y a otros remitidos por otras entidades públicas".[33] De lo anterior, afirma el juez constitucional, la UNP está obligada a cumplir con la Ley 1581 de 2012.

Los formularios de inscripción para el programa de prevención y protección, que entrega la UNP a los solicitantes de medidas de protección, incurren en deficiencias en materia de datos personales

Sea lo primero reparar en que la Ley 1581 de 2012 no dispone excepciones al principio de finalidad, según el cual el tratamiento de datos debe perseguir una finalidad legítima, así como tampoco hace distinción en el deber, a cargo del responsable del tratamiento, de informar al titular de la finalidad perseguida con la actividad de recolección, almacenamiento, uso, circulación o supresión.[34] En suma, de ser legítima, la jurisprudencia constitucional ha dispuesto que la finalidad también debe ser explícita, pertinente, atender a objetivos imperiosos y estar estrechamente relacionada con el tratamiento adelantado.

Tras examinar el acápite de consentimiento de los formularios de solicitud de medidas de protección en ruta individual y colectiva, se advierte que la finalidad informada al peticionario es confusa. Por una parte, se afirma que los datos recolectados tienen como fin "esta solicitud" y la "elaboración de estadísticas que se reflejarán en los ejercicios de caracterización e informes exigidos por Ley". Líneas más abajo, se lee que la información consignada en la solicitud se utilizará para "temas estadísticos y de caracterización poblacional". La redacción antes citada pone en entredicho la necesidad de la recolección de datos sensibles, pues admite utilizarlos para estadísticas e investigaciones que no guardan relación directa o indirecta con el objeto de la soli-

33. Corte Constitucional, Sentencia T-294 de 2023, M.P. Jorge Enrique Ibáñez Najar.
34. Ley 1581 de 2012, artículo 12, literal a); artículo 17, literal c).

citud de protección, y desatiende el mandato de la Corte Constitucional que dispone "debe hacerse todo lo razonablemente posible para limitar el procesamiento de datos personales al mínimo necesario".[35]

La UNP adelanta una actividad prohibida al exigir de los peticionarios de medidas de protección la entrega de datos personales sensibles

La Ley de Habeas Data proveyó una definición del dato sensible, refiriendo unas circunstancias –de carácter enunciativa y no taxativa– que están comprendidas en esta subclase de dato personal. El artículo 5° de la mentada ley establece que afectan la intimidad del titular del dato y por ende son sensibles "aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos."

Los formularios correspondientes a la proforma de inscripción para el programa de prevención y protección en ruta individual y colectiva respectivamente,[36] exigen para su debido diligenciamiento la entrega de datos personales sensibles como la afiliación partidista, la condición de reinsertado proveniente de la insurgencia, la pertenencia a organizaciones defensoras de los derechos humanos o la indicación de si se cuenta con alguna discapacidad visible o invisible. Lo anterior no podría realizarse sin la autorización explícita del titular del dato sensible en los términos del artículo 6°, literal a) de la Ley 1581 de 2012. Al respecto, la Corte Constitucional afirmó en la Sentencia C-748 de 2011 que "el dato sensible solamente podrá ser tratado para las finalidades expresamente autorizadas por el titular y que en todo caso deben ser importantes desde el punto de vista constitucional". En este sentido, y nada se menciona sobre el tratamiento diferenciado de datos sensibles en los lineamientos internos de la UNP, la entidad debe tener en consideración los parámetros específicos aplicables a este tipo de información para el cabal cumplimiento de la Ley de Habeas Data.

El tratamiento de datos adelantado por la UNP en el marco del programa de prevención y protección podría exceder una finalidad pertinente y necesaria

Examinado el Manual de políticas específicas de seguridad y privacidad de la información y los formularios de inscripción para el programa de prevención y protección,[37] así como el documento interno "Formato de orden de trabajo y reparto" entregados por la Unidad Nacional de Protección en el marco de esta investigación, se observa distintas formas de tratamiento de datos sensibles de peticionarios y beneficiarios

35. Corte Constitucional, Sentencia C-748 de 2011, M.P. Jorge Ignacio Pretelt Chaljub.
36. Formularios GSC-FT-11-V7 y GSC-FT-12-V5.
37. Formularios GSC-FT-11-V7 y GSC-FT-12-V5.

del programa de prevención y protección, adelantadas por individuos que prestan sus servicios a la UNP bien como trabajadores o como contratistas, éstos últimos sin siempre contar con el consentimiento previo y expreso del titular del dato. En punto de la pertinencia y necesidad del tratamiento, no se logra establecer el seguimiento del propósito de la actividad –tendiente a conceder o determinar la permanencia de una medida de protección–. Con este fin, debe constatarse la necesidad de recolectar, consignar y conservar información de los familiares del evaluado o protegido; de las discapacidades presentes en su núcleo familiar; de sus relaciones afectivas; de sus movimientos habituales, personales y laborales, así como de las rutas y horarios escogidos para los mismos.

El tratamiento de datos adelantado por la UNP en el marco del programa de prevención y protección parece ser indefinido en el tiempo porque no se indica la vigencia del mismo, por lo que es irrazonable e innecesario

El artículo 11° del Decreto 1377 de 2013 dispone una limitación temporal al tratamiento de datos, por "el tiempo que sea razonable y necesario, de acuerdo con las finalidades que justificaron el tratamiento, atendiendo a las disposiciones aplicables a la materia de que se trate y a los aspectos administrativos, contables, fiscales, jurídicos e históricos de la información".[38] Vistos los formularios y los documentos de gestión interna de la entidad, no se observa referencia alguna a la temporalidad del tratamiento de datos adelantado como parte del examen de la solicitud de protección. Podría interpretarse que la vigencia del mismo vencería al tiempo en que se profiere decisión de fondo, vía acto administrativo, sobre la solicitud de protección o sobre la revalidación de la medida otorgada, pero examinados los archivos antes mencionados se desconoce por cuánto tiempo conserva la UNP los datos personales ordinarios y sensibles que recolecta de los peticionarios y beneficiarios.

El tratamiento por parte de terceros distintos al encargado y al responsable de datos recolectados, almacenados, usados o circulados en el trámite de la solicitud de la medida de protección, bien sea durante o después del procedimiento, es ilícito si no cuenta con autorización previa y expresa del titular del dato para su transmisión

De acuerdo con informaciones que han circulado en la opinión pública, la UNP contrata a terceros para el cumplimiento de sus obligaciones legales.[39] Esta actividad es reconocida por la entidad en sus políticas internas al punto que comprende a los contratistas como sujetos disciplinables. En la política de transferencia de información, consignada en el Manual de políticas específicas de privacidad y seguridad de la información, se lee "[l]os servidores públicos, **contratistas y terceros autorizados**

38. Decreto 1377 de 2013, artículo 11.
39. La discusión en torno a la tercerización de los servicios ha sido constantemente discutida a la hora de evaluar el cumplimiento de las funciones de la UNP. Tómese, por ejemplo, el mensaje del director del Departamento Nacional de la Función Pública sobre la tercerización: https://www.unp.gov.co/a-los-trabajadores-de-la-unp/

no deben emitir copias, realizar divulgación o emplear indebidamente **datos e información** contenida en las aplicaciones, bases de datos y sistemas de información **a los cuales se les haya otorgado acceso,** con fines diferentes al cumplimiento de sus obligaciones" (subrayado fuera de texto).[40] Lo anterior, en la práctica, significa que, en las mismas condiciones que los funcionarios de la UNP, contratistas y terceros acceden a la información de la entidad. La cita en precedencia permite concluir que, en el marco de los procedimientos ordinarios de la entidad, se incurren en transmisiones de datos personales.

Si se tiene por cierto que el responsable del tratamiento de datos es la entidad a la cual le fue delegada la prestación del servicio de protección, es decir, la Unidad Nacional de Protección por mandato del Decreto 4912 de 2011, y si se admite la inferencia según la cual quien realiza el tratamiento es la dependencia asignada para el examen de las solicitudes al interior de la entidad –en el caso de ruta colectiva, el Cuerpo Técnico de Análisis de Riesgo Colectivo (CTARC) como se lee en el acápite de consentimiento del respectivo formulario–, cualquier actividad de transmisión de datos con terceros contratistas que no estén comprendidos como asociados al responsable o al encargado del tratamiento es contraria a la ley.

Los terceros contratistas de la UNP no están comprendidos como asociados al responsable o al encargado del tratamiento de datos recolectados en razón de la solicitud de protección

Vistos el Manual de políticas específicas de seguridad y privacidad de la información,[41] el acápite de consentimiento para el tratamiento de datos en el marco de la solicitud de medida de protección –en ambas rutas– y la Resolución 1848 del 26 de diciembre de 2016, que comprende la política de tratamiento de datos personales de la Unidad Nacional de Protección, no se evidencia que los terceros contratistas hayan sido reconocidos como responsables o encargados del tratamiento de datos recabados durante el trámite de las solicitudes de protección. Por tanto, cualquier transmisión lícita de éstos a aquellos exige una expresión de consentimiento explícito y previo del titular del dato, por cuanto dicho uso no estaría comprendido por la excepción legal que reviste a las entidades públicas en el ejercicio de sus funciones.[42]

En otras palabras, aunque la entidad sí puede tercerizar labores a su cargo, cuando se trata de la transmisión de datos de terceros debería mediar autorización expresa de los titulares de esos datos. Ante la ausencia de dicho aval, el uso de los datos por parte de aquellos terceros resulta ilegal.

El artículo octavo de la Resolución 1848 del 26 de diciembre de 2016, por medio del

40. Manual GTE-MA-02-V2, documento oficializado el 22 de junio de 2022.
41. Manual GTE-MA-02-V2, oficializado el 22 de junio de 2022.
42. Ley 1581 de 2012, artículo 6, literal a); artículo 10, literal a).

cual se establece que "[l]a Unidad Nacional de Protección solo podrá transmitir a los operadores de los servicios tercerizados datos personales que haya recolectado y tenga bajo su custodia, quienes suscribirán un contrato de transmisión de datos en los términos del artículo 2.2.2.25.5.2 del Decreto 1074 de 2015",[43] solo dimana los efectos pretendidos si se suscribe previo a la actividad de recolección desplegada por la entidad y si el titular de los datos está informado de la vinculación de este tercero, persona natural o jurídica, como asociado al tratamiento, de conformidad con lo previsto en el artículo 8°, literal e), y 12, literal d), de la Ley 1581 de 2012.

Por último, se repara en el hecho de que la competencia atribuida por virtud del artículo octavo de la precitada resolución está circunscrita al tratamiento de **datos recolectados y custodiados por la entidad,** por lo que el tercero asociado no estaría facultado para recabar y organizar datos por su cuenta, actividad que parece estar desplegando en la actualidad y que de hacerlo implicaría una transgresión a los principios de libertad y de acceso y circulación restringida consagradas en la Ley de Habeas Data.[44]

Los datos sensibles recolectados por la UNP no están categorizados, infringiendo el mandato del artículo 6° del Decreto 1377 de 2013

Vistos el Manual de políticas específicas de seguridad y privacidad de la información,[45] el acápite de consentimiento para el tratamiento de datos en el marco de la solicitud de medida de protección –en ambas rutas– y la Resolución 1848 del 26 de diciembre de 2016, atinente a la política de tratamiento de datos personales de la Unidad Nacional de Protección, no se encuentra instrucción ni mención al deber, a cargo del responsable o del encargado del tratamiento, de identificar y distinguir aquellos datos recolectados que revisten la naturaleza de sensibles, previsto en el numeral segundo del artículo sexto del Decreto 1377 de 2013. Como se ha mencionado, y de acuerdo a la normativa vigente, el tratamiento de datos sensibles sólo estará permitido bajo la autorización del titular. A su vez, según establece el artículo 6° del Decreto 1377 de 2023, se deberá i) informar al titular que, por tratarse de datos sensibles, no está obligado a autorizar el tratamiento y, ii) obtener el consentimiento expreso del titular, así como hacerle saber de forma explícita y previa cuáles de los datos objeto de tratamiento son sensibles y cuál es la finalidad del tratamiento.[46] El cumplimiento de estos lineamientos no se avizora en las políticas internas de la entidad.

El Manual de políticas específicas de seguridad y privacidad de la información no hace distinción entre información y dato personal, por lo que incurre en deficiencias respecto de éste último

43. Resolución 1848 del 26 de diciembre de 2016, artículo 8. Se anota que el Decreto 1074 de 2015 expide el Decreto Único Reglamentario del Sector Comercio, Industria y Turismo y no guarda relación con el régimen de habeas data.
44. Ley 1581 de 2012, artículo 4, literales c) y f).
45. Manual GTE-MA-02-V2, oficializado el 22 de junio de 2022.
46. Decreto 1377 de 2013, artículo 6.

De manera sostenida la entidad se refiere a la información como "activo", sin reparar en la naturaleza especial y objeto de mayor tutela judicial que reviste el dato personal. En punto de la política de medios removibles, por ejemplo, memorias; discos duros internos o externos, entre otros, dispone la norma que "[l]a responsabilidad de la información contenida en los medios removibles es del servidor público, contratista y terceros que está a cargo de este". Este precepto no se ajusta a la división de funciones y a la determinación de sujetos obligados (responsable y encargado del tratamiento de datos) prevista en la Ley 1581 de 2012, norma sustantiva de carácter estatutario y de orden público. Por su parte, la política de control de acceso no repara ni una sola vez en la protección reforzada que demanda la ley para el tratamiento de datos personales, así como tampoco distingue entre información, dato personal y dato sensible.

Ahora bien, la política de transferencia de la información incurre en un defecto incluso mayor. El literal e) del documento establece: "[e]s responsabilidad de los servidores públicos, contratistas y terceros autorizados no comprometer a la Entidad por difamación, acoso, suplantación, entre otros por la transferencia de información con fines personales o no autorizados". La disposición en cita parece dejar libre de consecuencias –disciplinarias o sancionatorias internas– el uso difamatorio, abusivo o defraudatorio de datos personales recabados por la entidad que no afecte la reputación o los intereses de la Unidad. Una redacción adecuada comprendería, como susceptible de procedimiento disciplinario o sancionatorio interno, cualquier utilización que exceda el propósito o la finalidad de la transferencia o del tratamiento de datos.

Por último, la política de seguridad de la información en las relaciones con los proveedores incluye una cláusula que se lee "[l]os servidores públicos y contratistas únicamente deben proporcionar acceso a la información de la Unidad Nacional de Protección – UNP a los proveedores cuando se requiera para cumplir con su objeto contractual, aplicando el principio de mínimos privilegios". Esta redacción desatiende por completo la obligación de (i.) obtener, previamente, consentimiento expreso del titular del dato personal para la transferencia del mismo a un tercero distinto al encargado o responsable del tratamiento, o, (ii.) celebrar un contrato de transferencia de datos con el tercero contratista previo a la actividad de recolección de datos por parte de la entidad.[47]

Tan evidente es la inobservancia de estas disposiciones y contradicciones que ante los hechos que llevaron a la Sentencia T-294 de 2023 -la solicitud de la periodista Claudia Julieta Duque de remover el dispositivo GPS del vehículo asignado por la inadvertencia de posible registro de sus movimientos sin su previa autorización- **la UNP afirmó que la información que se recolectaba por medio del dispositivo GPS,**

47. Resolución 1848 del 26 de diciembre de 2016, artículo 8.

"está relacionada con la puesta en marcha del vehículo, y en ningún momento se relaciona con datos personales de los beneficiarios".[48] A esta respuesta, el mencionado fallo establece que, mediante los dispositivos instalados en los vehículos asignados para la protección, la entidad obtiene y realiza un tratamiento de datos personales. En esta oportunidad, de acuerdo a la Corte Constitucional, la UNP vulneró el derecho al habeas data al rehusarse a entregar a la periodista la información solicitada sobre los datos recolectados sobre ella a través de mecanismos de monitoreo instalados en los vehículos asignados para su protección.[49]

EXPERIENCIAS SOBRE EL TRATAMIENTO DE DATOS PERSONALES POR PARTE DE LA UNIDAD NACIONAL DE PROTECCIÓN EN EL MARCO DEL PROGRAMA DE PROTECCIÓN

Ante las inconsistencias entre la normativa aplicable en materia de protección de datos personales y los lineamientos que sigue la Unidad Nacional de Protección se recopilaron varias experiencias que dan cuenta de un vacío de información importante durante el proceso de solicitud y adopción de las medidas de protección. Los nombres e información personal de los periodistas y personas consultadas se mantienen en reserva por motivos de seguridad, aunque su identidad ha sido amplia y suficientemente verificada por El Veinte, así como las notas correspondientes a sus entrevistas.

El viaje

Una de las periodistas contactadas por El Veinte para esta investigación relató un hecho de la mayor gravedad, por

48. Corte Constitucional, Sentencia T-294 de 2023, M.P. Jorge Enrique Ibáñez Najar.
49. Ibíd.

antecederle una seguidilla de hostigamientos, amenazas y atentados por parte de funcionarios públicos: la protegida viajó fuera del país por compromisos laborales, pero en razón de su precaria situación de seguridad y atendiendo al hecho de que uno de sus familiares cercanos tendría protección de la UNP durante su ausencia decidió mantener en secreto la información de su vuelo de regreso a Colombia. Sin embargo, previo a su vuelo el escolta asignado recibió una llamada de un individuo desconocido, quien se presentó como funcionario de la UNP y le dio todos los datos de identificación tanto de la periodista como de su familiar, así como la información del vuelo en el que arribaría aquella, a efectos de que él se presentara en el aeropuerto para recogerla.

La situación descrita anteriormente da cuenta de una actividad inadvertida de recolección y tratamiento de datos personales sensibles, sin autorización de su titular y en abierta contravención del principio de libertad. Si bien la recolección de información sensible por parte de la UNP –en cumplimiento de sus obligaciones legales– está exenta de la obligación de contar con consentimiento previo y expreso de su titular, toda actividad de tratamiento de datos debe atender a una finalidad legítima, explícita y pertinente. También debe estar estrechamente vinculada al objetivo de la base de datos, ser necesaria, almacenarse por un término razonable y necesario, e informada previa y expresamente al titular la categorización de datos sensibles comprendidos por la actividad de tratamiento.

La conducta antes descrita contradice el mandato del juez constitucional según el cual "debe hacerse todo lo razonablemente posible para limitar el procesamiento de datos personales al mínimo necesario",[50] considerando que la beneficiaria de la medida de protección decidió libre, consciente y voluntariamente conservar para sí la información de su vuelo de regreso, por lo que tal dato –que por su naturaleza y por la calidad de su titular constituye dato personal sensible– no debió hacer parte de la actividad de tratamiento a cargo de la UNP, además, por no ser necesaria ni pertinente ni atender a una finalidad legítima e imperiosa.

Quien calla no otorga

Los periodistas beneficiarios de medidas entrevistados para esta investigación coincidieron en que la UNP no informó sobre la actividad de tratamiento de datos entregados por el peticionario con ocasión de la solicitud de protección; ni sobre la actividad de recaudación y procesamiento de datos recaudados durante la vigencia de la medida; así como tampoco hizo explícitas las finalidades perseguidas con ambas actividades.

50. Corte Constitucional, Sentencia C-748 de 2011, M.P. Jorge Ignacio Pretelt Chaljub.

El régimen legal de protección de datos no prevé excepción a los principios de finalidad y transparencia, por lo que toda actividad de tratamiento debe atender una finalidad legítima y además impone una carga a su responsable o encargado relativa a "[i]nformar debidamente al [t]itular sobre la finalidad de la recolección y los derechos que le asisten por virtud de la autorización otorgada"[51], cuya exigibilidad no está atada a previa solicitud del titular del dato. Dado que la información sobre la finalidad del tratamiento es una obligación ex ante y ex post y surge como consecuencia de la actividad de recolección; almacenamiento; uso; circulación; supresión o demás afines al tratamiento de datos personales, la UNP incumplió con su deber de información y vulneró el derecho de los beneficiarios entrevistados a ser notificados tanto de su calidad de titulares de datos como de los derechos que les corresponden.

En un caso puntual, una periodista que ha sido beneficiaria de esquemas asignados tanto por el Departamento Administrativo de Seguridad (DAS) como por la UNP manifestó que, con la entrada en funcionamiento de esta última y la transferencia de competencias por parte del DAS, no hubo notificación alguna de la transmisión de información a la UNP, aun cuando está acreditado que hoy la poseen. Incluso, a pesar de lo establecido en el Decreto Ley 4057 de 2011 -por medio del cual se suprime el DAS- en su artículo 3° que consagra el traslado de funciones y le asigna al Ministerio de Defensa y a la Policía Nacional el deber de garantizar "que la información contenida en las bases de datos mantenga los niveles de seguridad requeridos de acuerdo a su naturaleza".[52] Esta conducta no sería admisible conforme a la normativa vigente, puesto que las actividades de transferencia y transmisión de datos personales exigen, de no mediar un contrato de transmisión de datos personales en los términos del artículo 25° del Decreto 1377 de 2013, del consentimiento del titular.

La varada

Un periodista que es también beneficiario de medidas de protección relató un hecho que indica la reducida protección que efectúa la UNP respecto de los datos personales sensibles: cuenta que por temor a la divulgación de la información entregada a la entidad, decidió proveer solo una de sus dos direcciones de residencia. Un día, el vehículo asignado al esquema presentó una falla y no pudo movilizarse, por lo que hubo de contactar a la entidad para que enviaran una grúa. Al llamar a la dependencia encargada, el funcionario dio la información exacta de la ubicación del vehículo, sin que hubiere manifestación previa de ésta por parte del protegido o de sus escoltas. Tiempo después el periodista conoció de la presencia de un dispositivo de geolocalización instalado en el vehículo provisto por la UNP, sin su consentimiento ni conocimiento, y reparó en que desde el día de la falla –y posterior solicitud de asistencia a la entidad–

51. Ley 1581 de 2012, artículo 17, literal c).
52. Decreto Ley 4057 de 2011, artículo 3.

en los archivos de su medida en la UNP reposa la dirección en que ocurrió el hecho antes descrito como una de sus direcciones de residencia, aun cuando él no la informó en la primera solicitud de protección ni en las entrevistas ni en los posteriores procedimientos de reevaluación del riesgo.

La presencia desconocida –y por tanto inconsulta y no consentida– de un dispositivo que recaba, conserva e informa la ubicación en tiempo real del vehículo de protección, sumado a la completa indeterminación del responsable y del encargado del tratamiento de estos datos; así como de la finalidad perseguida con esta actividad, torna en improcedente e irregular el procedimiento de recolección, almacenamiento, uso, circulación o supresión de datos por medio de este elemento y vicia de ilegalidad la información que de éste se haya sucedido.

Para agravar el estado de cosas, la facilidad con que el operario que atendió la llamada accedió al dato sensible relativo a la geolocalización del vehículo lleva a creer que la información custodiada por la UNP y obtenida por medio del GPS es de fácil acceso por parte de los funcionarios de esta entidad, situación indeseada toda vez que se trata de información que de divulgarse sitúa en grave riesgo al titular del dato, considerando que el hecho que origina la actividad de tratamiento de datos es la imposición de una medida de protección por haberse acreditado un riesgo extraordinario contra la vida e integridad personal del beneficiario.

La Corte Constitucional ha avalado este tratamiento de datos a la luz de la Sentencia T-294 de 2023 por considerar que el sistema de monitoreo en el vehículo “cumple con un juicio estricto de proporcionalidad”, incluso sin contar con la autorización expresa del titular. El Veinte disiente de esta postura y, en todo caso, considera que el uso de este dispositivo debe darse de forma limitada, con priorización del consentimiento como fundamento legal y bajo unos parámetros de limitación en la finalidad y de minimización de la información. Asimismo, el fallo de la Corte Constitucional, que exhorta a la UNP a velar por el “estricto cumplimiento de su política de tratamiento de datos” deja pasar los vacíos en los mismos lineamientos de la entidad.

Sobre el caso en concreto de la Sentencia T-294 de 2023, la periodista Claudia Julieta Duque, alegó la vulneración a sus derechos a la intimidad, habeas data, libertad de expresión, libertad de profesión y oficio, seguridad y dignidad humana pues en su vehículo se había instalado un dispositivo GPS sin su autorización. La vulneración permaneció cuando la UNP se negó a retirar el dispositivo y a eliminar los datos relacionados de los registros de la entidad, así como a entregar información completa sobre lo que la accionante identificó como “actos de seguimiento y espionaje”. Sobre esto, la Corte Constitucional consideró que, a pesar de no contar con su consenti-

miento, el tratamiento de los datos recolectados en el dispositivo GPS cumple con una finalidad legal y permitida, en últimas, sirve para la protección. Para la eventual evaluación de remoción, el fallo señala que la periodista tendrá que demostrar que la información recolectada por el mecanismo de monitoreo se le ha dado un uso inadecuado o ilegal. Se difiere de esta postura porque, además de pasar por alto consideraciones sobre la política interna de protección de datos personales de la UNP a la luz de la regulación de habeas data, este tipo de medidas, que recopilan datos de alta sensibilidad como la localización de personas en riesgo, pueden resultar exageradamente invasiva en relación con los beneficios que representan y aumentar el riesgo de perfilamientos sobre los movimientos de los beneficiarios.

Sin lugar para el disenso

Uno de los periodistas entrevistados para esta investigación relató que tras la negativa de la UNP a pagar viáticos en favor de sus dos escoltas –erogación que le corresponde hacer por cuanto no puede imputarse a cargo de éstos los desplazamientos de su protegido– formuló una petición a la entidad para que explicara los motivos de su decisión. Días después de promover la petición, el periodista fue informado de una "revisión de uso" de la medida de protección a él asignada, la cual no había sido programada con anterioridad ni correspondía al término anual de revaluación del estado de riesgo. El beneficiario de la medida concluyó razonablemente que se trataba de una represalia al hecho de haberse, en sus palabras, "revolucionado".

La conducta antes desplegada comporta una infracción al principio-derecho de moralidad administrativa, que debe orientar el ejercicio de la función administrativa conforme a criterios de buena fe, ética, honestidad y satisfacción del interés general. No se descarta que, como consecuencia de la decisión de revisar el uso de la medida extemporáneamente y sin motivo fundado, se haya incurrido en una malversación de recursos del erario, potencialmente constitutiva de delito.

¿Para qué tantos datos?

La Fundación para la Libertad de Prensa (FLIP), organización con amplio conocimiento sobre el procedimiento de evaluación y determinación de la concesión de medidas de protección por parte del Comité de Evaluación del Riesgo y Recomendación de Medidas (CERREM), manifestó que en el acto administrativo que resuelve si se asigna la protección no se explica en forma detallada el uso, valoración y contrastación de la información personal proveída en el marco del trámite de solicitud. Esta indeterminación deviene en una potencial infracción al régimen legal de habeas data, por cuanto es un derecho del titular del dato "ser informado [...], previa solicitud, respecto del uso

que le ha dado a sus datos personales". De solicitar la explicación del uso a la entidad y ser rechazada o no contestada, se efectuaría la vulneración al derecho.

¿Dónde guardan los datos?

Conocida la presencia de dispositivos de geolocalización a bordo de vehículos asignados como parte del programa de protección a personas, la FLIP, según relata en entrevista, se puso a la tarea de encontrar quién era el receptor de los datos recabados por medio de éstos y halló que la información es recibida por una empresa radicada en Estados Unidos, quien la conserva en servidores situados en ese país y respecto de la cual se desconoce si existe un contrato para la transmisión de datos con la Unidad Nacional de Protección. De igual manera, no existe indicación alguna relativa a los funcionarios de la entidad que pueden acceder a esta información y no se hace ningún reparo a este respecto en el Manual de políticas específicas de seguridad y privacidad de la información. Finalmente, no se conoce si en la transferencia de datos en este caso cumple con lo establecido en la Ley 1581 de 2012 sobre "transferencia de datos personales a terceros países".

El dato a merced del contratista

La circunstancia descrita antes muestra al menos tres infracciones al régimen legal de protección de datos: por una parte, a los escoltas –en tanto contratistas independientes– no se les extiende la excepción al deber de contar con consentimiento previo, expresa y específico respecto del tratamiento de datos, al no pertenecer a la entidad facultada para adelantarlo sin anuencia del titular. En segundo lugar, si bien pueden existir contratos de transmisión de datos personales con las compañías de seguridad privada contratadas para prestar el servicio de seguridad humana, tales no facultan necesariamente a éstas para desempeñar por su cuenta actividades de recolección de información salvo que la UNP lo delegue expresamente, de conformidad con lo previsto en el artículo 25° de la Ley 1581 de 2013, que se lee: "[e]l contrato [...] señalará [...] las actividades que el encargado realizará por cuenta del responsable para el tratamiento de los datos personales" (negrilla fuera de texto).[53]

Por último, dado que la única calidad por la que las empresas de seguridad pueden tener acceso a información recabada durante la vigencia de una medida de protección es a título de parte contratista en un contrato de transmisión de datos celebrado por la UNP, aquellas están obligadas a salvaguardar y guardar confidencialidad respecto de los datos, deberes que parecen incumplirse. No debe pasarse por alto que al contratista encargado del tratamiento por vía de contrato de transmisión le son

53. Ley 1581 de 2013, artículo 25.

exigibles todas las obligaciones, deberes y sanciones contempladas en la ley para el encargado, además de las que se dispongan en el contrato antes referido.

La policía de los datos

La Fundación para la Libertad de Prensa relató la experiencia de los solicitantes que, en razón de su situación de seguridad, se ven precisados a solicitar una medida de protección transitoria, vigente durante el examen de su petición. Manifestó que en ejecución de ésta, la autoridad a cargo de su aplicación –a saber, la Policía Nacional– inspecciona regularmente los exteriores al domicilio del beneficiario, solicita de éste su firma en caso de que se halle en la vivienda y de lo contrario, deja constancia en una "planilla" de que no se encuentra en casa. Asimismo, comentó que es frecuente que los policías tomen fotos a la residencia, cuyo uso, destinación, finalidad y custodia es desconocida.

La presencia de la Policía Nacional en el programa de protección a personas suscita varios inconvenientes. En primera medida, se desconoce si la UNP ha suscrito contratos de transmisión de datos personales, pues ésta sería la única vía lícita para que la Policía adelante un tratamiento en el marco del programa. En segundo lugar, si las conductas de recolección de información antes referidas son indispensables para el cumplimiento de la medida transitoria, es probable que se incurra en la expresa prohibición legal de supeditar una actividad "a que el Titular suministre datos personales sensibles"[54] como lo son, por ejemplo, la localización; la ubicación del domicilio privado y la relación de movimientos o desplazamientos.

Como tercera observación, a diferencia de la UNP, la Policía Nacional puede reclamar la excepción al régimen legal de protección de datos consagrado en la Ley 1581 de 2013, por cuanto integra la fuerza pública y desempeña labores que pueden subsumirse en la cláusula de excepción por "bases de datos y archivos que tengan por finalidad la seguridad y defensa nacional".[55] Sin desmedro de lo anterior, conviene recordar que de conformidad con el precedente jurisprudencial originado en la Sentencia C-748 de 2011, aun en hipótesis de excepción al régimen legal de protección de datos cualquier actividad relativa a éstos debe sujetarse a los principios contenidos en el artículo 4° de la citada ley, por corresponder a "garantías mínimas de protección del habeas data". Por último, preocupa –por inconveniente, poco fiable y difícil de mantener en confidencialidad– la práctica de recolección de información por medio de planillas diligenciadas a mano, en las que se consignan datos de la mayor sensibilidad y que es posible que sean accesibles a otros ciudadanos por hallarse en dicho formato.

54. Decreto 1377 de 2013, artículo 6.
55. Ley 1581 de 2013, artículo 2, literal b).

CONCLUSIONES

Si bien tanto la regulación general en materia de habeas data y privacidad en términos generales, como los lineamientos específicos de la Unidad Nacional de Protección sobre tratamiento de datos personales establecen un marco normativo relativamente completo especialmente durante el proceso de solicitud de las medidas de protección, en la práctica, los beneficiarios carecen de suficiente protección para el efectivo cumplimiento de sus derechos a la privacidad y a la seguridad digital.

En todo caso, como se evidencia en las comunicaciones de la UNP así como en la experiencia de los beneficiarios, hay poca o nula claridad sobre el tratamiento de sus datos personales durante la adopción, seguimiento y evaluación de la medida de protección. Aún más, la UNP tampoco es clara sobre lo que considera o no un dato personal de un beneficiario y confunde la información de las personas en riesgo a quienes, por mandato legal debe proteger, con aquella relativa al mero funcionamiento de las medidas de protección.

De esta manera, no hay certeza en la práctica de la correcta aplicación del Manual de políticas específicas de seguridad y privacidad de la información en relación con las obligaciones y principios de la Ley de Habeas Data, mucho menos hay una consideración aterrizada sobre los efectos de este descuido tanto en la garantía a la privacidad y seguridad digital de los usuarios, como al cumplimiento mismo de los fines de la medida de protección a la integridad, libertad y seguridad personal.

Es así cómo, si bien podría considerarse que una política interna que se alinee a las disposiciones generales de privacidad y habeas data es favorable para la garantía de los derechos de los usuarios, también hace falta que se implementen medidas para la entrega de información, actualización y seguimiento en materia de recolección, almacenamiento, acceso y eliminación de la información personal. De lo anterior se desprenden las siguientes recomendaciones para el fortalecimiento del cumplimiento de los lineamientos de privacidad para la Unidad Nacional de Protección y, en general, para la recolección de información tecnológica en cabeza del Estado:

- La política interna de la UNP para la privacidad, tratamiento de datos personales y seguridad digital debe ser comprensiva de la integralidad del proceso de solicitud, adopción y evaluación de las medidas de protección. No basta con alinearse con las disposiciones generales de habeas data si la regulación de la entidad no tiene en cuenta que, además de los datos recolectados al momento de la solicitud, durante la adopción y evaluación de las medidas de protección también tiene la entidad una deber legal sobre la información registrada en esas etapas. Adicionalmente, la UNP debe ajustar sus lineamientos a lo establecido en la regulación sobre el tratamiento de datos sensibles. En este sentido, debe i) contar siempre con la autorización del titular para el tratamiento de datos sensibles ii) informar al titular que, por tratarse de datos sensibles, no está obligado a entregar la autorización para el tratamiento, iii) informar al titular, tras obtener el consentimiento expreso, cuáles de los datos objeto de tratamiento son datos sensibles y cuál es la finalidad del tratamiento.

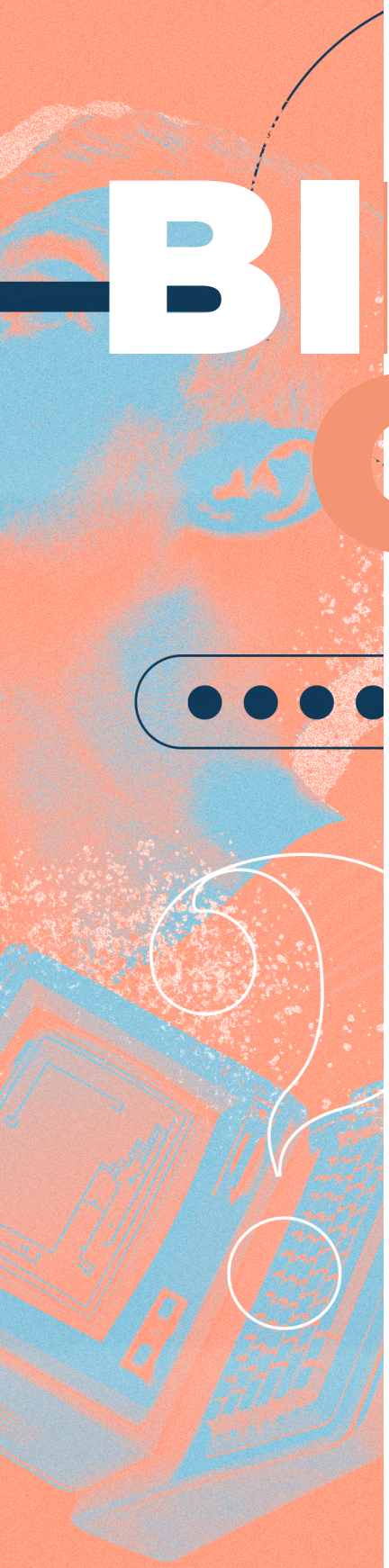
- La UNP debe ser clara y diligente en la entrega de información sobre el tratamiento de datos personales en el procedimiento de solicitud, adopción y evaluación de las medidas de protección. Esto es especialmente importante para aquellos usuarios con medidas de protección implementadas previamente a la creación de la UNP que, según se registró en las entrevistas realizadas para esta investigación, afirman no conocer sobre el traslado de la información desde otras entidades. Asimismo y en cumplimiento de la Sentencia T-294

- de 2023, estas medidas deben contar con lineamientos para la actualización y seguimiento en materia de recolección, almacenamiento, uso, circulación o supresión de información personal, así como una evaluación de la finalidad del tratamiento y revisión de los controles establecidos para el cumplimiento de la Política de Tratamiento y Protección de Datos Personales de la UNP, siempre que se alinee con los estándares normativos vigentes.

- En particular sobre los dispositivos de monitoreo instalados en los vehículos de los esquemas de protección, incluso si la Corte Constitucional avaló su uso en la Sentencia T-294 de 2023, se considera que su uso solo debe ser procedente bajo la autorización expresa del beneficiario y en los casos limitados en los que la UNP pueda demostrar la función para la protección que supere lo invasivo de la medida.

- En concordancia con los estándares internacionales sobre privacidad y protección de datos personales, se recomienda a la UNP evaluar la posibilidad de minimizar y limitar el tratamiento de datos personales a lo estrictamente necesario para el cumplimiento de su finalidad. Esta medida, además de la reducción de riesgos en el manejo de la información y las garantías al cumplimiento del habeas data, logra agilizar los procesos internos de la entidad para el fortalecimiento de la eficacia administrativa.

- Finalmente, se recomienda considerar la adopción de un reglamento aplicable, en términos más amplios que los lineamientos internos de la UNP, a la recolección de información tecnológica en cabeza del Estado.



BIBLIOGRAFÍA

Comisión Interamericana de Derechos Humanos, Relatoría Especial para la Libertad de Expresión, "Violencia contra periodistas y trabajadores de medios: Estándares interamericanos y prácticas nacionales sobre prevención, protección y procuración de la justicias", 2013, https://www.oas.org/es/cidh/expresion/docs/informes/2014_04_22_Violencia_ESP_WEB.pdf

Congreso de la República de Colombia. Constitución Política de Colombia (1991).

Congreso de la República de Colombia. Ley 1581 de 2012: "Por la cual se dictan disposiciones generales para la protección de datos personales", (Diario Oficial No. 48.587 de 2012).

Consejo de Estado, Sala de lo Contencioso Administrativo, Sentencia del 8 de junio de 2011, C.P. Jaime Orlando Santofimio Gamboa [radicado n.° 25000-23-26-000-2005-01330-01(AP)]

Corte Constitucional, Sentencia T-1037 de 2008, M.P. Jaime Córdoba Triviño.

Corte Constitucional, Sentencia C-748 de 2011, M.P. Jorge Ignacio Pretelt Chaljub.

Corte Constitucional, Sentencia T-294 de 2023, M.P. Jorge Enrique Ibáñez Najar.

Corte Interamericana de Derechos Humanos, Bedoya Lima y otra v. Colombia, Sentencia de 26 de agosto de 2021. Serie C No. 431, párr. 152

Corte Interamericana de Derechos Humanos, Defensor de derechos humanos v. Guatemala, Sentencia de 28 de agosto de 2014. Serie C No. 283, párr. 263

Entrevista a la Fundación para la Libertad de Prensa, coordinación de protección. Realizada el 1 de junio de 2023.

Entrevista a periodista beneficiaria 1. Realizada el 11 de septiembre de 2023.

Entrevista a periodista beneficiario 2. Realizada el 12 de septiembre de 2023.

Fundación para la Libertad de Prensa (FLIP), "Páginas para la libertad de expresión", Quinta Edición, 2023, https://flip.org.co/publicaciones/informes/quinta-edicion-paginas

Naciones Unidas, Relatoría Especial sobre el derecho a la privacidad del Alto Comisionado para los Derechos Humanos, "Principios que informan la privacidad y la protección de datos personales", A/77/196, 2022, https://www.ohchr.org/es/documents/thematic-reports/a77196-principles-underpinning-privacy-and-protection-personal-data

Presidencia de la República. Decreto 4065 de 2011: "Por el cual se crea la Unidad Nacional de Protección (UNP), se establecen su objetivo y estructura" (31 de octubre).

Presidencia de la República. Decreto Ley 4057 de 2011: "Por el cual se suprime el Departamento Administrativo de Seguridad (DAS), se reasignan unas funciones y se dictan otras disposiciones" (31 de octubre).

Presidencia de la República. Decreto 4912 de 2011: "Por el cual se organiza el Programa de Prevención y Protección de los derechos a la vida, la libertad, la integridad y la seguridad de personas, grupos y comunidades del Ministerio del Interior y de la Unidad Nacional de Protección" (26 de diciembre).

Presidencia de la República. Decreto 1377 de 2013: "Por el cual se reglamenta parcial-

mente la Ley 1581 de 2012" (27 de junio).

Presidencia de la República. Decreto Único Reglamentario 1066 de 2015: "Por medio del cual se expide el Decreto Único Reglamentario del Sector Administrativo del Interior" (26 de mayo)

Presidencia de la República. Decreto 1066 de 2015: "Por medio del cual se expide el Decreto Único Reglamentario del Sector Administrativo del Interior" (13 de septiembre)

Reporteros sin frontera, "Clasificación: Puntuación Global", 2023, https://rsf.org/es/clasificacion

Unidad Nacional de Protección. Resolución 1848 de 2016: "Por la cual se adopta La Política de Tratamiento y Protección de Datos Personales de la Unidad Nacional de Protección" (26 de diciembre).

Unidad Nacional de Protección. Reglamento del Comité de Evaluación del Riesgo y Recomendación de Medidas.

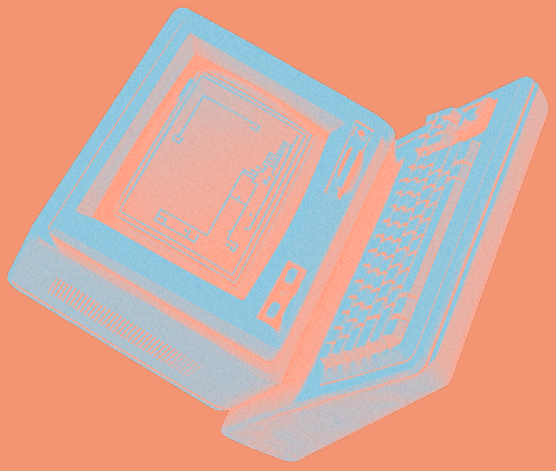
Unidad Nacional de Protección. Formulario de inscripción para el programa de prevención y protección en ruta individual (Formulario GSC-FT-11-V7).

Unidad Nacional de Protección. Formulario de inscripción para el programa de prevención y protección en ruta colectiva (Formulario GSC-FT-12-V5).

Unidad Nacional de Protección. Formato de orden de trabajo y reparto.

Unidad Nacional de Protección. Manual de políticas específicas de seguridad y privacidad de la información (Manual GTE-MA-02-V2, oficializado el 22 de junio de 2022).

2023



EL VEINTE