https://doi.org/10.18800/iusetveritas.202501.005

Actividades de inteligencia, intimidad y habeas data: una sistematización de los estándares de derechos humanos(*)

Intelligence activities, privacy, and habeas data: a systematization of human rights standards

Rodrigo Uprimny Yepes(**)
Universidad Nacional de Colombia (Bogotá, Colombia)

Resumen: El artículo propone, a partir de una revisión de fuentes jurídicas internacionales, tanto del sistema universal de derechos humanos, como del europeo y americano y, en especial, de la sentencia CAJAR contra Colombia de la Corte Interamericana de Derechos Humanos, una sistematización de los estándares de derechos humanos que permitan armonizar las actividades de inteligencia. Estas son necesarias para las democracias, pero riesgosas para los derechos por su carácter reservado, con los derechos a la intimidad, al acceso de información y al habeas data que, en ciertos ordenamientos y textos, suele ser denominado derecho a la autodeterminación informativa. El texto presenta tanto estándares normativos como institucionales y, en particular, enfatiza que no bastan los controles judiciales, sino que es necesario que existan instituciones independientes civiles para el monitoreo y control de las actividades de inteligencia.

Palabras clave: Actividades de Inteligencia - Habeas Data - Privacidad - Autodeterminación Informativa - Instituciones de Monitoreo y Control - Archivos de Inteligencia - Derecho Internacional de los Derechos Humanos - Colombia

Abstract: Based on a review of international legal sources from both the universal human rights system and the European and American human rights systems, in particular, the decision CAJAR vs Colombia of the Interamerican Human Rights Court, the article proposes a systematization of human rights standards that allows for the harmonization of intelligence activities. These are necessary for democracies but pose risks to human rights due to their confidential nature, with the rights to privacy, access to information, and habeas data. In particular, the article presents both normative and institutional standards, notably pointing out that judicial oversight is not sufficient; independent civilian institutions are necessary to monitor and control intelligence activities.

Keywords: Intelligence Activities - Habeas Data - Privacy - Informational Self-determination - Monitoring And Control Institutions - Intelligence Files - International Human Rights Law - Colombia

(*) Nota del Equipo Editorial: Este artículo fue recibido el 02 de junio de 2025 y su publicación fue aprobada el 04 de enero de 2026.
(**) Abogado por la Universidad Externado de Colombia (Bogotá, Colombia). Doctor en Economía Política por la universidad de Amiens Picardie. Maestría en Socioeconomía del desarrollo de la Universidad de París I. Profesor principal de la Universidad Nacional de Colombia. Investigador senior del Centro de Estudios de Derechos, Justicia y Sociedad "Dejusticia". ORCID: https://orcid.org/0000-0003-0943-5417. Correo electrónico: ruprimny@dejusticia.org.

1. Introducción

Una de las discusiones más difíciles y más relevantes en filosofía política y en derechos humanos es la relativa al siguiente dilema: ¿qué tanto poder y atribuciones debe otorgársele a las autoridades, a fin de que sean eficaces y puedan lograr el orden y la paz? Y, de otro lado, ¿qué tantos controles y límites deben imponérsele a esas mismas autoridades a fin de que no abusen su poder? Uno de los padres fundadores del constitucionalismo estadounidense, James Madison, expresó en términos impecables y que siguen siendo relevantes este dilema, por lo cual sus palabras ameritan ser recordadas. En el Federalista 51, Madison dijo lo siguiente:

> Si los hombres fueran ángeles, no sería necesario ningún gobierno. Si los ángeles gobernaran a los hombres, no serían necesarios controles externos ni internos al gobierno. Al organizar un gobierno que debe ser ejercido por hombres sobre hombres, la mayor dificultad reside en esto: primero debe facultarse al gobierno para controlar a los gobernados y en segundo lugar obligarlo a que se controle a sí mismo (Hamilton, Madison y Jay, 1948, p. 279).

Aunque hoy, por obvias razones de género, hablaríamos de gobiernos de personas y no de hombres, el dilema señalado por Madison sigue siendo relevante porque los seres humanos no somos ángeles y los gobernantes tampoco lo son.

Este dilema adquiere un particular dramatismo al regular las facultades y controles de las actividades y organismos de inteligencia. Las operaciones de inteligencia son necesarias para que los Estados democráticos puedan detectar a tiempo y enfrentar adecuadamente grandes amenazas, como el terrorismo o el crimen organizado, pero también los organismos que las desarrollan se han visto involucrados en algunas de las peores violaciones a los derechos humanos. Además, por el sigilo y secreto en que inevitablemente realizan sus labores, los organismos de inteligencia son difícilmente controlables. Estamos frente a unas actividades que son necesarias en las democracias y pueden producir grandes beneficios, pero que, igualmente, son muy riesgosas y muy difíciles de controlar.

Por todo lo anterior, es muy importante desarrollar, aclarar y sistematizar los estándares y criterios de derechos humanos que permitan una regulación democrática de las actividades de inteligencia; en especial, en su relación con dos derechos que podrían verse particularmente afectados por ese tipo de operaciones. Dado su necesario sigilo: la intimidad y el llamado *habeas data* que, algunos autores y tribunales, prefieren denominar el derecho a la autodeterminación informativa o derecho a la protección de los datos personales (Moreno y Serrano, 2021; Mendoza, 2021). Este artículo busca avanzar en esa dirección, aprovechando que el autor fue perito en este tema en el caso más importante de la Corte Interamericana de Derechos Humanos (en adelante, Corte IDH). Así, sobre estos aspectos, nos referimos al caso "Miembros de la Corporación Colectivo de Abogados "José Alvear Restrepo" vs. Colombia", que condujo a la sentencia del 18 de octubre de 2023, de ahora en adelante, sentencia CAJAR[(1)].

El artículo retoma entonces los criterios y argumentos que presenté en mi peritaje en ese caso, muchos de los cuales -lo digo con orgullo- fueron incorporados por la Corte IDH en la citada sentencia CAJAR. La reconstrucción de ese peritaje bajo la forma de artículo académico se justifica y no representa una indebida autocitación, a pesar de que retomo literalmente pasajes del peritaje, por cuanto no solo el texto del peritaje es de difícil acceso, sino que, además, un artículo académico tiene diferencias importantes con el lenguaje más forense propio de un peritaje. Son géneros literarios diversos.

El artículo comienza, en la primera parte, con una reflexión abstracta y filosófica, pero muy relevante para el tema: los papeles opuestos y complementarios que juegan el secreto y la transparencia en una democracia. La segunda parte presenta las bases normativas del análisis: el status de los derechos a la privacidad y del acceso a la información y a documentos públicos en el derecho internacional, lo cual me permitirá, en una tercera parte, sustentar la tesis de la existencia del *habeas data* como derecho humano, la cual fue acogida, aunque con un lenguaje diverso -derecho a la autodeterminación informativa-, por la Corte IDH en la citada sentencia CAJAR. Esto me permitirá entonces mostrar, en una cuarta parte, las tensiones entre las operaciones de inteligencia y estos derechos a la intimidad, al acceso a la información y al *habeas data*

(1) Las citas formales de las sentencias de la Corte IDH son innecesariamente largas y complejas. Esta sentencia CAJAR es formalmente citada así: Corte IDH, Caso Colectivo de Abogados "José Alvear Restrepo" (CAJAR) vs. Colombia, Excepciones Preliminares, Sentencia de 18 de octubre de 2023, Serie C No. 506. Por eso, para aligerar el texto, en este artículo me refiero de manera más informal esas sentencias de la Corte IDH o del Tribunal Europeo de Derechos Humanos, pues considero que basta con citar la fecha y el caso para que puedan ser totalmente identificadas por los lectores, que es lo que busca una referencia bibliográfica.

y presentar los principales documentos internacionales que han intentado buscar una armonización entre esos derechos y las operaciones de inteligencia, y que podrían operar como fuentes jurídicas de *soft law* en este estudio.

El análisis teórico, la fundamentación normativa y la recopilación de esas fuentes jurídicas me permiten, en la quinta parte, desarrollar la contribución esencial de este artículo: una propuesta de sistematización de los principios y estándares de derechos humanos, tanto formales y sustantivos como procesales e institucionales, que permiten armonizar las operaciones de inteligencia con la protección de los derechos a la privacidad y al habeas data. La conclusión resalta las contribuciones esenciales de este artículo y termina con unas breves reflexiones sobre la relevancia de esos aportes para América Latina, dados los desafíos particulares que enfrentan nuestros países en este tema por cuanto requerimos de organismos de inteligencia eficaces -dados nuestros agudos problemas de seguridad- pero es igualmente una región en que estos organismos se han visto involucrados en atroces violaciones a los derechos humanos.

2. Una visión filosófica general: transparencia y secreto en una democracia robusta y respetuosa de la dignidad humana(2)

Una democracia robusta y una efectiva protección de la dignidad humana requieren articular lo que podríamos denominar el juego de espejos entre la transparencia pública y la penumbra de la vida privada, a fin de que logremos proteger tanto la autonomía individual como la autodeterminación colectiva.

De un lado, la libertad no germina en una sociedad que pretenda la transparencia total y el fin de todos los secretos, pues toda persona requiere de ámbitos íntimos en donde pueda, en la penumbra hogareña, sin la presión constante de las miradas ajenas, construir un proyecto de vida propio. La razón es clara: la libertad personal y una autonomía genuina solo pueden florecer si se protegen espacios libres de la intromisión ajena y en donde puedan brotar planes individuales de vida. La absoluta transparencia destruye la diversidad y provoca una empobrecedora uniformidad de los comportamientos, las ideas y las personalidades. Sin una cierta opacidad en los espacios íntimos es incluso difícil que se desarrolle una verdadera solidaridad entre las personas, pues el otro no es visto como aquél con quien compartimos dignidad, proyectos e ilusiones, sino que aparece como el portador de esa mirada que nos inmoviliza. El otro es el carcelero que coarta nuestra espontaneidad y, paradójicamente, nosotros somos a su vez su carcelero.

Estos riesgos de estar sometidos a la mirada ajena permanente los expresó maravillosamente Jean Paul Sartre en su obra de teatro "*A puerta cerrada"*, en la cual uno de los personajes centrales, Garcin, luego de darse cuenta de que en el infierno no hay fuegos ni torturas físicas sino la obligación de estar permanentemente en un cuarto sometido a al escrutinio y al juicio de otras personas, concluye lo siguiente: "el infierno son los otros porque sus miradas nos devoran" (1971, p 92).

La absoluta transparencia a la contemplación del otro no es entonces la realización de la libertad y la solidaridad entre las personas sino todo lo contrario: un paraíso totalitario semejante al descrito por Georges Orwell, en *1984*, en donde el valor mismo del proceso democrático pierde su sentido: ¿De qué sirve un amplio y libre flujo de ideas si estas han sido uniformizadas por la presión constante de la mirada de los otros y del Estado?¿Qué utilidad puede tener la autodeterminación colectiva si los integrantes del cuerpo social no tienen la capacidad de ser libres en tal proceso? Es más, incluso la "libertad política, por ejemplo, a través del voto, requiere una cierta soledad. La gente no vota libremente cuando los demás saben lo que vota. La cabina electoral cumple la función de conservar ese secreto" (García, 1992, p 20). No puede existir entonces un proceso político libre y una sociedad democrática si no se garantiza una órbita de secreto y de intimidad a las personas. Por paradójico que suene, solo si tenemos espacios de soledad, secreto y autonomía, estaremos en capacidad de construir comunidades solidarias, humanas y democráticas.

De otro lado, sin una discusión abierta, transparente y vigorosa sobre los asuntos colectivos, no podemos garantizar una

(2) Esta parte retoma parcialmente, actualiza y ajusta las reflexiones realizadas en un artículo escrito hace 25 años, pero que considero pertinente retomar, pues no solo tengo gran aprecio por esos apartes, sino que, además, creo que son de clara relevancia en este tema. Para ello, *véase* "La uni-diversalidad de los derechos humanos: conflictos de derechos, conceptos de democracia e interpretación constitucional", de Rodrigo Uprimmy (1998).

vigilancia ciudadana sobre los gobiernos, ni una genuina autonomía colectiva, las cuales presuponen la existencia de una opinión pública libre e informada. El espacio público es entonces central para materializar el Estado de derecho y la democracia, que precisamente pretende ser un gobierno en público, esto es, transparente, de la esfera pública, esto es, de aquel ámbito en donde se discuten los asuntos que a todos nos conciernen e interesan. Por ello, y con el fin de insistir en esa doble dimensión y significación de lo público, no parece exagerado definir a la democracia, como lo hizo Norberto Bobbio, como el "gobierno del poder público en público" (1994, p. 65).

La transparencia y la publicidad de los debates sobre los asuntos de interés general cumplen entonces en el Estado de derecho y en la democracia finalidades esenciales, como lo sostienen las concepciones sobre la democracia deliberativa(3). La publicidad racionaliza la discusión colectiva y la hace más receptiva a los distintos intereses y opiniones en la sociedad, con lo cual las deliberaciones producen resultados más adecuados y aceptables. La transparencia de lo público es incluso necesaria para la propia justicia de las decisiones, ya que existen argumentos y motivos que pueden invocarse a puerta cerrada pero que no son admisibles al hacerse públicos, pues su injusticia se vuelve manifiesta. Por ello, Kant consideraba que uno de los principios trascendentales del derecho público era el siguiente: "son injustas todas las acciones que se refieren al derecho de otros hombres cuyos principios no soportan ser publicados" (1985, p 61).

La deliberación pública permite así un mayor control ciudadano sobre las autoridades, con lo cual realiza en forma más profunda los ideales del Estado de derecho y de la soberanía popular, pues obliga a los funcionarios a justificar y explicar sus decisiones. Finalmente, esta discusión pública de los asuntos comunes estimula la formación de virtudes republicanas en los ciudadanos y en los líderes políticos, en la medida en que los obliga a ir más allá de sus intereses puramente personales. En una democracia deliberativa, en la medida en que las decisiones se fundan en una discusión pública, los ciudadanos y los líderes tienen que defender sus posiciones con base en argumentos con una pretensión de universalidad suficiente para que sus tesis puedan ser aceptados por todos los eventualmente afectados, o al menos puedan ser presentados públicamente.

La opinión pública en una democracia no debería entonces ser el promedio estadístico de las creencias y preferencias individuales que las personas tienen en privado, sino que, debe ser una opinión cualificada, que resulta de un debate colectivo vigoroso, el cual puede incluso llevar a los sujetos a modificar sus creencias y preferencias originarias. Por todas esas razones, la transparencia de los asuntos colectivos aparece como un requisito necesario para que exista un verdadero ejercicio de la autodeterminación colectiva, que es la esencia de la democracia, ya que las personas no podrían participar en la toma de decisiones si no se encuentran informadas sobre los asuntos generales y pueden debatirlos libremente.

La publicidad es además uno de los mejores mecanismos de control a los eventuales atropellos de los gobernantes, ya que el temor al escándalo y a las protestas ciudadanas inhiben a las autoridades de cometer conductas contrarias a los principios que sustentan la legitimidad del orden social. Citando nuevamente a Bobbio, el escándalo "es el momento en el que se hace público un acto o una serie de actos que hasta ese momento se habían mantenido en secreto y escondidos, en cuanto no podían ser hechos públicos porque, si esto sucedía, tal acto o serie de actos no hubieran podido ser realizados" (1994, p. 71). La discusión pública de los asuntos colectivos juega entonces funciones morales, epistemológicas, de control de los abusos gubernamentales y de autodeterminación social esenciales.

La experiencia histórica también ha demostrado que, sin un control democrático a los gobiernos, es muy difícil proteger la intimidad y la autonomía de las personas frente a los gobiernos y a las miradas ajenas. La transparencia de la esfera pública y la autodeterminación colectiva son entonces un requisito para preservar la penumbra de los hogares y las esferas de privacidad en donde las personas construyen sus proyectos individuales. Como lo señala Hannah Arendt:

> El dominio público, mundo común, nos reúne, pero igualmente nos impide, por expresarlo de esa manera, caer los unos sobre los otros. Lo

(3) Sobre estas visiones, *v*éase, entre otros, los textos "Deliberative Democracy" de James Bonham y William Rehg (1997), "Between facts and norms. Contributions to a discourse theory of law and democracy" de Jürgen Habermas (1995) y "La constitución de la democracia deliberativa" de Carlos Santiago Nino (1997).

> que hace que la sociedad de masas sea tan difícil de soportar no es principalmente el número de personas; es que el mundo que hay entre ellas no tiene el poder de reunirlas, de ligarlas, ni de separarlas. Extraña situación que evoca una sesión de espiritismo en la cual los participantes, víctimas de un pase mágico, vieran de pronto desaparecer la mesa, con lo cual las personas sentadas las unas en frente de las otras no estarían ya separadas, pero tampoco entrelazadas por nada tangible (1983, pp. 92 - 93).

Existe entonces un juego de diferenciaciones y complementariedades entre las zonas de penumbra privada y la transparencia de los debates públicos. Por ello, como lo ha planteado Hannah Arendt, lo público y lo privado no están gobernadas por los mismos principios, sino que responden a orientaciones diversas, ya que la distinción entre esas esferas "equivale a la diferencia entre lo que debe y puede ser mostrado -lo visible- y lo que puede y debe ser ocultado" (Laffer, 1991, p. 293). El espacio público debe estar gobernado por la igualdad en la participación, la transparencia y la verdad, pues constituye aquel lugar en donde se discuten los asuntos que nos interesan a todos. En lo privado operan otros principios, ya que aquí la situación solo atañe a una persona o a unos pocos, por lo cual rige lo que Arendt (1983) llama el principio de exclusividad. En este ámbito, que debe entonces estar sujeto a la reserva, buscamos construir las particularidades de nuestra propia vida.

La transparencia y la opacidad son entonces complementarias en una democracia constitucional: la protección de la dignidad humana y la participación democrática exigen tanto la luz en la esfera pública, como las sombras en la vida íntima, ya que solo de esa manera podemos proteger la autonomía, la autenticidad y la libertad de las personas. La aspiración democrática es entonces que los ciudadanos sean verdaderamente soberanos y que puedan entonces ver permanentemente a los gobernantes sin ser vistos por ellos. En cambio, el totalitarismo invierte los anteriores principios. El secreto se instala en las estructuras de poder, mientras que los individuos son sometidos a la permanente mirada de los otros y de la autoridad. El gobernante logra ver sin ser visto, mientras que el gobernado es visto sin poder ver, con lo cual se destruye al mismo tiempo la esfera de lo público y la esfera de lo privado, la autodeterminación colectiva y la autonomía individual.

Esta reflexión sobre la penumbra y la transparencia en la democracia es esencial para nuestro análisis pues permite reformular el dilema planteado en la introducción en la siguiente forma: ¿cómo lograr que las operaciones de inteligencia en una democracia sean eficaces para enfrentar los grandes desafíos de seguridad, pero evitando que esas actividades, que por esencia son reservadas y pueden interferir en la privacidad de las personas, conduzcan a formas de totalitarismo? Una respuesta posible es a través de la sistematización de estándares de derechos humanos adecuados en este campo, que es lo que intento desarrollar en los siguientes puntos.

3. El fundamento normativo: privacidad, acceso a la información y a documentos públicos en el derecho internacional

La anterior visión sobre el lugar de la privacidad y la esfera pública en una democracia explica que los tratados de derechos humanos y las constituciones democráticas protejan, al mismo tiempo y en forma robusta, el derecho a la vida privada y su reserva y el derecho de acceso a la información pública. Procedo entonces a presentar esos dos fundamentos normativos de mi análisis.

La protección de la vida privada y su reserva tienen consagración expresa en las Declaración Universal de Derechos Humanos (artículo 12), en la Declaración Americana de los Derechos y Deberes Del Hombre (artículo 5) y en los principales tratados de derechos humanos, como la Convención Americana de Derechos Humanos [CADH] en su artículo 11, el Pacto de Derechos Civiles y Políticos [PIDCP] en su artículo 17 y el Convenio Europeo de Derechos Humanos [CEDH] en su artículo 8. Su reconocimiento no plantea entonces particulares controversias. Por el contrario, el derecho de acceso a la información contenida en archivos públicos no tiene un fundamento textual claro en los instrumentos internacionales de derechos humanos y por ello, hasta hace unos veinte años, su estatus jurídico internacional podía suscitar alguna controversia. Incluso un tribunal tan agudo como el Tribunal Europeo de derechos humanos [TEDH], en algunos casos, como en la sentencia "Guerra contra Italia" de 1998, negó que los Estados tuvieran una obligación positiva de suministrar a quien los solicitara los documentos en su posesión pues consideró que su deber era tan solo garantizar que las personas pudieran recibir la información que otros quisieran suministrarles: que el derecho a recibir información prevista en el artículo 10 sobre libertad de expresión del CEDH imponía únicamente una obligación negativa, pues prohibía que el Estado interfiriera en la posibilidad de que una persona recibiera la información que otro individuo quisiera

suministrarle, pero no imponía ninguna obligación positiva al Estado[4].

Este precario reconocimiento del derecho a la información y a acceder documentos públicos cambió profundamente entre 2006 y 2012: en esos años, tanto el sistema interamericano como los sistemas universal y europeo reconocieron explícitamente el derecho a la información, que incorpora igualmente un derecho de acceder a los documentos contenidos en archivos públicos[5].

En este importante avance el sistema interamericano tuvo la iniciativa: la Corte IDH, en el caso Claude Reyes vs. Chile de 2006, fue la primera instancia internacional de derechos humanos en reconocer claramente el derecho de acceso a la información, el cual implica una obligación positiva del Estado de suministrarle a las personas la información en su poder, salvo que existan razones justificadas para limitar el acceso a esa información. El párrafo esencial es el 77, que conviene transcribir *in extenso*, en el cual dice entonces la Corte IDH:

> En lo que respecta a los hechos del presente caso, la Corte estima que el artículo 13 de la Convención, al estipular expresamente los derechos a "buscar" y a "recibir" "informaciones", protege el derecho que tiene toda persona a solicitar el acceso a la información bajo el control del Estado, con las salvedades permitidas bajo el régimen de restricciones de la Convención. Consecuentemente, dicho artículo ampara el derecho de las personas a recibir dicha información y la obligación positiva del Estado de suministrarla, de forma tal que la persona pueda tener acceso a conocer esa información o reciba una respuesta fundamentada cuando por algún motivo permitido por la Convención el Estado pueda limitar el acceso a la misma para el caso concreto. Dicha información debe ser entregada sin necesidad de acreditar un interés directo para su obtención o una afectación personal, salvo en los casos en que se aplique una legítima restricción. Su entrega a una persona puede permitir a su vez que esta circule en la sociedad de manera que pueda conocerla, acceder a ella y valorarla. De esta forma, el derecho a la libertad de pensamiento y de expresión contempla la protección del derecho de acceso a la información bajo el control del Estado, el cual también contiene de manera clara las dos dimensiones, individual y social, del derecho a la libertad de pensamiento y de expresión, las cuales deben ser garantizadas por el Estado de forma simultánea (2006, p. 43).

Por su parte, desde 2009, el TEDH fue variando su jurisprudencia al respecto. Así, en la sentencia Kenedi vs. Hungría de ese año, el TEDH reconoce que la negativa del Estado a suministrar documentos en su poder equivale a una interferencia en la libertad de recibir información del artículo 10 del CEDH. Esta evolución jurisprudencial se consolida con la decisión de la Grand Chamber del TEDH en el caso Gillberg vs. Suecia de 2012, en la que ese tribunal, en los párrafos 94 y 95, reconoce la existencia del derecho de acceso a documentos públicos, como componente de la libertad de expresión.

Finalmente, el Comité de Derechos Humanos, en el ámbito universal, también reconoció el derecho de acceso a información pública como componente de la libertad de expresión. Primero lo hizo en varios dictámenes frente a peticiones individuales particulares, como en el caso Toktakunov vs. Kyrgyzstan de 2006, para luego señalarlo en forma más general en su Observación General No 34 de 2011 sobre el artículo 19 del PIDCP sobre libertad de expresión. El Comité dice expresamente en el párrafo 18 de dicha Observación General lo siguiente:

> El párrafo 2 del artículo 19 enuncia un derecho de acceso a la información en poder de los organismos públicos. Esta información comprende los registros de que disponga el organismo público, independientemente de la forma en que esté almacenada la información, su fuente y la fecha de producción (2011).

Conforme a lo anterior, es claro entonces que hoy está reconocido en el derecho internacional de los derechos humanos no solo el derecho a la protección de la vida privada sino también el derecho a acceder a los documentos en poder de las autoridades.

---

(4) En ese caso, los peticionarios consideraban que la negativa del Estado italiano de proveerles información sobre los riesgos de la operación de una empresa que podía causar daños sanitarios desconocía el artículo 10 del CEDH sobre derecho a recibir información. El TEDH negó la petición pues consideró que el artículo 10 no era aplicable y señaló explícitamente, en el párrafo 54, que "la libertad de recibir información básicamente prohibía al gobierno restringir información que otros quisieran proveerle, pero esa libertad no podía ser interpretada como imponiendo al Estado, en circunstancias como las del caso, una obligación positiva de recolectar y diseminar información sobre su propia dinámica" (traducción personal del original en inglés).

(5) Sobre esta evolución, *véase* los siguientes textos: "The right to information in international human rights law" de Maeve McDonagh (2013), "Artículo 13: libertad de expresión" de Eduardo Bertoni, Daniela Salazar Marín y Carlos J. Zelada (2019) y "El derecho a la libertad de expresión: Curso avanzado para jueces y operadores jurídicos en las Américas" de Catalina Botero Marino, Federico Guzmán Duque, Sofía Jaramillo Otoya y Salomé Gómez Upegui (2017).

4. Acceso a la información sobre datos personales, autodeterminación informativa y fundamentación del *habeas data* como derecho humano

El derecho general de acceso a la información pública debe ser entendido como un derecho humano intrínseco o en sí mismo considerado, por lo cual opera, como lo dijo explícitamente la Corte IDH en el párrafo 77 del caso Claude Reyes vs. Chile, sin que la persona deba mostrar una particular legitimación o interés para ejercerlo pues la "información debe ser entregada sin necesidad de acreditar un interés directo para su obtención o una afectación personal, salvo en los casos en que se aplique una legítima restricción". En el mismo sentido, el Comité de Derechos Humanos, en su citada Observación General 34, en el párrafo 18, no condicionó ese derecho a que la persona tenga un interés especial para obtener esa información. Es pues un derecho autónomo. Sin embargo, esto no significa que sea irrelevante que la información contenida en archivos estatales pretendida por la persona sea necesaria para amparar o realizar intereses esenciales u otros derechos humanos; en esos casos debe entenderse que la fuerza normativa del derecho de acceso a los documentos en poder del Estado se ve reforzada, por lo cual aún más limitadas son las posibilidades del Estado de negar esa información.

Este vínculo reforzado del acceso a la información cuando están en juego otros derechos o intereses puede verse en los desarrollos jurisprudenciales de los tres sistemas. En el sistema universal, el Comité de Derechos Humanos, en casos como Gauthier vs. Canadá, decidido en 1999, mostró el vínculo estrecho entre el derecho de acceso a la información y el derecho de participación pues encontró una violación del PIDCP debido a la negativa del Estado canadiense a permitir a un periodista que accediera a información de debates parlamentarios, que luego pudiera divulgar públicamente.

Por su parte, el TEDH, en casos como K.H. y otros vs. Eslovaquia, decidido en 2009, mostró las relaciones entre el derecho de acceso a la información y otros derechos, como la protección de la vida privada y el acceso a la justicia, pues señaló que a unas mujeres Roma les habían violado sus derechos por cuanto les negaron la posibilidad de fotocopiar sus archivos médicos, para ver si habían sido esterilizadas sin su consentimiento y poder eventualmente reclamar una reparación por esos hechos. La ratio de esa sentencia es que las personas tienen derecho a acceder a archivos que contengan sus datos personales y por consiguiente las autoridades tienen menores posibilidades de limitar el acceso en esos casos.

Finalmente, la Corte IDH, en el caso Gomes Lund y otros (guerrilha do Araguaia) vs. Brasil de 2010, fuera de reiterar la doctrina del caso Claude Reyes vs. Chile sobre el derecho de acceso a la información, mostró igualmente su vínculo con el derecho a la verdad de las víctimas y sus familiares en casos de graves violaciones a los derechos humanos. En el párrafo 202 de esa sentencia, la Corte IDH señaló que el derecho a la información se ve reforzado en esas circunstancias y concluyó:

> En casos de violaciones de derechos humanos, las autoridades estatales no se pueden amparar en mecanismos como el secreto de Estado o la confidencialidad de la información, o en razones de interés público o seguridad nacional, para dejar de aportar la información requerida por las autoridades judiciales o administrativas encargadas de la investigación o proceso pendientes (2010).

Igualmente, la Corte IDH precisó en ese párrafo que

> Cuando se trata de la investigación de un hecho punible, la decisión de calificar como secreta la información y de negar su entrega jamás puede depender exclusivamente de un órgano estatal a cuyos miembros se les atribuye la comisión del hecho ilícito (2010).

Ese vínculo del derecho de acceso a la información con otros derechos permite entonces fundamentar la existencia del *habeas data* en el derecho internacional de los derechos humanos, o un derecho a la protección de los datos personales contenidos en bases de datos o archivos, especialmente si estos están bajo control del Estado. El contenido de ese derecho es entonces, en términos generales, el siguiente: toda persona tiene derecho a acceder a los datos que se refieran a ella contenidos en esas bases de datos y, en caso de que sea procedente, puede solicitar su modificación, si son equivocados, o su supresión, si afectan el derecho a la vida privada.

El *habeas data* resulta entonces de una articulación entre la protección de la vida privada, el derecho a la honra y el derecho de acceso a la información. O, por decirlo metafóricamente, de una fundamentación combinada a partir de los artículos 11 y 13 de la CADH o de los artículos 17 y 19 del PIDCP.

Esta articulación de esos derechos parece, a primera vista, paradójica ya que la protección de la vida privada exige reserva, mientras que el derecho de acceso a la información se fundamenta en los principios de publicidad y transparencia. Sin embargo,

el *habeas data* adquiere pleno sentido como protección de la privacidad si se tiene en cuenta que las sociedades contemporáneas han sido caracterizadas como "sociedades digitales" o "sociedades de la información", en que la información, debido a la revolución digital y de las comunicaciones, puede ser recolectada, almacenada y circulada como nunca antes en la historia humana(6). En el mundo contemporáneo, una de las formas de proteger la intimidad es entonces que la persona tenga control sobre los datos e informaciones sobre su vida privada que estén contenidos en bases de datos o archivos y que puedan ser objeto de la mirada de los otros y de las autoridades. Por eso toda persona debe tener acceso a esos datos y poder controlar que no desconozcan su intimidad ni su honra. La protección de los datos personales es considerada hoy entonces como un componente esencial de la protección de la vida privada y de la honra.

El habeas data como derecho humano o derecho fundamental -sin importar si se acoge o no esa denominación, que es usual en ciertos países latinoamericanos, debido a la constitucionalización del habeas data en las últimas décadas en la región (Puccinelli, 2004), pero que es una expresión menos utilizada en otros contextos regionales, como el europeo, en donde se habla mayormente del derecho a la protección de los datos personales- ha sido reconocido explícitamente en el sistema universal. En efecto, el Comité de Derechos Humanos, en la citada Observación General No 34, señala que, cuando el derecho de acceso a la información está ligado a la protección a la privacidad, existe una especie de habeas data como derecho humano internacional. Dice explícitamente el Comité:

> (…) Algunos elementos del derecho a acceder a la información se encuentran también en otras disposiciones del Pacto. Como señaló el Comité en su Observación general No. 16, en relación con el artículo 17 del Pacto, 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 sus 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 que se rectifiquen esos datos (párr. 18, 2011).

Aunque tampoco usa la expresión, esa misma idea es desarrollada por el TEDH, que reconoce que el derecho de acceso a la información se ve reforzado cuando protege el acceso a datos personales, como lo muestra el ya referido caso K.H. y otros vs. Eslovaquia, decidido en 2009 y varios otros, como los siguientes: Leander vs. Suecia decidido en 1987, Gaskin vs. Reino Unido, decidido en 1989 o Rotaru vs. Rumania, decidido en 2000 por la Grand Chamber o Odièvre vs. Francia decidido en 2003 igualmente por la Grand Chamber.

El sistema interamericano, hasta la citada sentencia CAJAR, no había señalado explícitamente al *habeas data* como derecho humano en nuestro sistema regional. La posible razón de esa falta de reconocimiento explícito es que hasta ese momento la Corte IDH no había tenido que abordar un asunto relacionado con el acceso de datos personales en archivos o bases de datos, que fue uno de los temas centrales de la sentencia CAJAR.

Ese caso fue entonces la oportunidad para que la Corte IDH desarrollara el contenido del *habeas data* como derecho humano interamericano, como lo recomendé en mi peritaje, en el entendido de que ese derecho es una consecuencia lógica de la jurisprudencia de la Corte IDH sobre acceso a la información, en especial en los precedentes ya citados de los casos Claude Reyes c Chile y Gomes Lund vs. Brasil, cuando se relaciona el acceso a la información con la protección de la vida privada y la honra, esto es, cuando los artículos 11 y 13 de la CADH son interpretados en forma articulada y sistemática. La particularidad del sistema interamericano es que igualmente habría que tomar en consideración el artículo 25 sobre recurso judicial efectivo en esta fundamentación, no solo porque una interpretación sistemática de la CADH, acorde con la jurisprudencia interamericana, así lo impone jurídicamente sino, además, por cuanto resulta esencial, en nuestro sistema, que las personas puedan eventualmente acudir ante un juez en caso de que resulten insuficientes los mecanismos no judiciales para garantizar el habeas data, que también deberían prever los ordenamientos nacionales, como el reclamo directo ante quien posee el archivo o la base de datos y la previsión de un mecanismo administrativo de protección. Con razón, expertos en el tema, como Upegui Mejía (2019), han resaltado

(6) Sobre la relevancia del concepto de sociedad de la información para repensar los problemas de protección de datos personales, *v*éase "The right to privacy in the digital age" del Alto Comisionado de las Naciones Unidas (2014).

la importancia de que exista esa triada de mecanismos para proteger el habeas data: reclamo directo, reclamo ante autoridad administrativa y protección judicial.

En la citada sentencia CAJAR, la Corte IDH, en los párrafos 585 a 600 reconoce explícitamente el *habeas data*, que denomina "derecho a la autodeterminación informativa" y precisa que es un derecho autónomo que resulta sustantivamente de la articulación de los derechos previstos en los artículos 11 -honra, intimidad y privacidad- y 13 -libertad de expresión y derecho de acceso a la información- de la CADH; y que igualmente requiere la protección judicial prevista en el artículo 25 de ese mismo tratado. La Corte IDH, en el párrafo 585, precisa entonces que este derecho de toda persona a acceder y controlar los datos suyos que consten en archivos públicos se compone analíticamente de los siguientes cinco derechos específicos:

> (i) el derecho a conocer qué datos se encuentran en los registros de los órganos públicos, en soportes físicos, magnéticos, electrónicos o informáticos, de dónde provienen, cómo fueron obtenidos, para qué son utilizados, el plazo de su conservación, si son compartidos con otras instancias o personas, la razón de ello y, en general, las condiciones de su tratamiento;(ii) el derecho a reclamar la rectificación, modificación o actualización de los datos, en el caso de ser inexactos, incompletos o no estar actualizados; (iii) el derecho a exigir la eliminación, cancelación o supresión de los datos, en caso de constatar la ilegalidad de su recopilación o conservación, o la inexistencia de razones que justifiquen su mantenimiento en archivos o bases de datos estatales, en tanto ello no afecte otros derechos, lo que necesariamente debe ser ponderado en orden a la naturaleza de los archivos de que se trate y la información que contienen, siempre de acuerdo a la regulación aplicable; (iv) el derecho a oponerse al tratamiento de los datos, en los casos en que, en razón de la situación particular de la persona, se cause un daño en su perjuicio, así como en los supuestos que la normativa sobre la materia disponga, y (v) cuando fuere posible y de acuerdo a las previsiones legales pertinentes, el derecho a recibir los datos en un formato estructurado, de uso común y lectura mecánica, y requerir su transmisión sin que lo impida la autoridad que los conserva.

Dos comentarios finales sobre esta fundamentación y reconocimiento expreso del *habeas data* en el derecho interamericano de derechos humanos. Primero sobre la denominación de este derecho. La Corte IDH, en la nota 760 de la sentencia CAJAR, adopta un lenguaje distinto al desarrollado en este artículo pues considera que el *habeas data* no es el derecho sustantivo sino la vía judicial o garantía procesal para asegurar "la efectiva protección del derecho a la autodeterminación informativa, que constituye el elemento material o sustantivo que es objeto de protección, precisamente, de aquella garantía". Algo semejante a la relación que, según ciertas visiones, existe entre el *habeas corpus* y la libertad física: el habeas corpus sería la garantía o mecanismo procesal para proteger la libertad física, que sería el derecho fundamental.

Esa opción de lenguaje de la Corte IDH, que es considerada acertada por ciertos autores (Puccinelli, 2004), es razonable y tal vez terminará por imponerse en el derecho interamericano, por la autoridad jurídica de ese tribunal. Sin embargo, en este artículo he preferido mantener, al menos temporalmente, la denominación de *habeas data* para este derecho, que adopté en el peritaje y que ha sido más aceptada por ciertos doctrinantes (Cifuentes, 1997) y por ciertos tribunales constitucionales, como el colombiano(7), porque encuentro que la expresión "habeas data" tiene ciertas virtudes lingüísticas frente a aquella del "derecho a la autodeterminación informativa": mayor brevedad, cierta belleza y enfatiza la importancia de la dimensión procesal para la efectiva protección de los datos personales.

Segundo, algunos podrían objetar que el reconocimiento del *habeas data* como derecho humano en el sistema interamericano es una contribución pobre o menor de la sentencia CAJAR y de este artículo y de mi peritaje, por cuanto el derecho a la autodeterminación informativa y la protección de datos personales ya estaban ampliamente desarrollados en el derecho europeo y en múltiples ordenamientos jurídicos latinoamericanos. Este posible reparo parte de un hecho cierto, pero infiere

(7) Por ejemplo, *véase* la sentencia C-748 de 2011, en la cual la Corte Constitucional colombiana revisó integralmente la constitucionalidad del proyecto que daría lugar a la Ley Estatutaria 1581 de 2012 sobre protección de datos personales. La Corte reiteró que el derecho fundamental al *habeas data*, que es la denominación asumida por la jurisprudencia constitucional colombiana, era equivalente al derecho a la autodeterminación informativa reconocido en otros ordenamientos jurídicos.

(8) Sobre estos desarrollos, *véase*, entre otros, los siguientes textos: "Derecho fundamental a la protección de los datos personales en América Latina: desafíos ante el alcance extraterritorial del Reglamento General de Protección de Datos de la Unión Europea" de Francisco Sanz Salguero (2025), "El derecho a la protección de datos personales en Europa y en América: Diferentes visiones para una misma realidad" de Ángela Moreno Babadilla y María Isabel Serrano Maillo (2021) y "El derecho de protección de datos personales en los sistemas de inteligencia artificial" de Olivia Andrea Mendoza Enríquez (2021).

una conclusión equivocada. Es cierto que en los últimos años numerosos países latinoamericanos y europeos desarrollaron importantes normatividades internas para la protección de datos personales y que, además, la Unión Europea desarrolló regulaciones comunitarias en esa dirección(8)

Sin embargo, hasta ahora la existencia del *habeas data* no había sido claramente sustentada en el sistema interamericano de derechos humanos, por lo cual se trata de una clara e importante innovación jurisprudencial. Además, es un avance sólido ya que se basa en una interpretación al mismo tiempo textual (la referencia a los artículos 11, 13 y 25 de la CADH), como evolutiva y finalista: el *habeas data* es reconocido porque es visto como necesario porque la garantía de la privacidad, el buen nombre y la autonomía en el mundo digital y de la información contemporáneo requiere que las personas puedan tener un mecanismo efectivo que les permita controlar la información que sobre ellas está contenida en archivos y bases de datos.

5. Derechos a la privacidad y a la honra, habeas data y actividades de inteligencia: tensiones y esfuerzos de armonización

Una vez recordadas la existencia de los derechos a la privacidad y al acceso a la información y fundamentada la existencia del *habeas data* en el derecho internacional, especialmente pero no exclusivamente, en el derecho internacional interamericano, entro a analizar su relación y sus tensiones con las actividades de inteligencia.

Las labores de inteligencia, sean policiales o militares, persiguen propósitos trascendentales, como son la protección de la seguridad pública y nacional, por lo cual su existencia está justificada en un Estado democrático. Sin embargo, una de las características de esas actividades es que se realizan, en muchos aspectos, en forma reservada y pueden implicar vigilancias secretas sobre los ciudadanos, por lo cual, a pesar de los importantes fines que persiguen, estas labores de inteligencia representan riesgos considerables de abuso contra los derechos de las personas o de desvío de esas labores a otros fines, como la persecución de la oposición política. Por eso, como lo ha dicho el TEDH en numerosas sentencias, desde su ya clásico caso Klass vs. Alemania Federal de 1979, esas labores de vigilancia secreta a los ciudadanos solo son admisibles en la medida en que sean estrictamente necesarias para preservar las instituciones democráticas(9). Conforme a su doctrina del margen de apreciación, el TEDH ha reconocido que las autoridades nacionales tienen una cierta discrecionalidad para organizar en distintas formas y con diversa amplitud esos servicios de inteligencia y sus competencias pero que, en todo caso, las interferencias en la vida privada deben estar "basadas en razones relevantes y suficientes y deben ser proporcionadas al objetivo perseguido"(10).

Igualmente, la Corte IDH, en el párrafo 527 de la sentencia CAJAR, y basada en numerosos casos previos, insistió en que, dada la reserva en que se desarrollan las actividades de inteligencia, sin conocimiento del público en general y sin el consentimiento de quienes podrían verse directamente afectados, aumenta considerablemente "el riesgo de un ejercicio abusivo del poder público".

En este contexto, existe una obvia tensión normativa y práctica entre el *habeas data*, que establece que las personas tienen derecho a acceder a la información personal contenida en archivos estatales, e incluso que el Estado no pueda tener mis datos personales sin mi consentimiento, y las actividades de inteligencia estatales, las cuales, como hemos visto, exigen altas dosis de secreto y reserva y por ello implican naturalmente recolección de información sobre los ciudadanos sin su consentimiento. Por ello es necesario encontrar mecanismos y garantías que armonicen la protección de la privacidad y del *habeas data* frente a las actividades de inteligencia.

En este aspecto, considero que existen al menos seis importantes desarrollos doctrinarios y jurisprudenciales comparados que buscan armonizar las labores de inteligencia con la protección de la privacidad y el habeas data por cuanto esos seis tipos de documentos formulan principios bastante coincidentes sobre el alcance del *habeas data* y del derecho de acceso a la información frente a esas actividades.

(9) Al respecto, *véase*, entre otras, el párrafo 42 de la sentencia del TEDH en el caso Klass y otros vs. Alemania de 1979; o el párrafo 47 del caso Rotaru vs. Rumania, decidida en 2000; o el párrafo 88 del Caso Segersted-Wiberg y otros vs. Suecia de 2006.

(10) Para una mayor profundización respecto a este apunte del TEDH, *véase* el Caso Segersted-Wiberg y otros vs. Suecia de 2006, con especial énfasis en el párrafo 88.

Primero, encontramos los llamados "Principios de Johannesburgo" o, usando su denominación completa, los "Principios de Johannesburgo sobre seguridad nacional, libertad de expresión y acceso a la información"(11). Estos principios fueron adoptados en 1995 por un grupo de expertos internacionales reunidos en Johannesburgo bajo la coordinación de la conocida organización de derechos humanos sobre libertad de expresión "ARTICLE 19", el "International Centre Against Censorship" y la Universidad de Witwatersrand. Aunque no son en sí mismos vinculantes, estos principios han adquirido una importante autoridad jurídica como documento de *soft law* en esta materia, no solo por su fuerza doctrinaria de origen sino, además, por su evolución posterior. De un lado, los expertos que los formularon los entendieron esencialmente como principios de *lege lata* y no como de *lege ferenda*: consideraron que no eran propuestas acerca de cómo debería regularse el tema, sino que representaban una sistematización de los estándares internacionales de derechos humanos ya existentes en la materia. De otro lado, posteriormente esos principios han sido apoyados en distintos informes por los relatores de la libertad de expresión de Naciones Unidas, fueron invocados en varias sesiones por la entonces Comisión de Derechos Humanos y han sido tomados en cuenta por diversas cortes nacionales(12). Finalmente, la Corte IDH, en el citado caso CAJAR, los toma en consideración.

Segundo, encontramos las que podríamos denominar "buenas prácticas Scheinin", que están basadas en el importante informe de 2010 al Consejo de Derechos Humanos del entonces Relator Especial de Naciones Unidas sobre promoción y protección de los derechos humanos y las libertades fundamentales en la lucha contra el terrorismo, Martin Scheinin. Este informe recopila y sistematiza, después de una amplísima consulta a los Estados y a distintos actores interesados, las buenas prácticas desarrolladas por los Estados para garantizar que las actividades de inteligencia respeten los derechos humanos (Sheinin, 2010). Este informe no pretende formular explícitamente principios normativos sobre las labores de inteligencia ya que es una recopilación de buenas prácticas, tal vez la más completa que se haya hecho hasta la fecha. Por eso, como dice el propio relator, el informe usa un lenguaje descriptivo y no uno prescriptivo.

Sin embargo, este informe del relator Scheinin, al sistematizar esas 35 buenas prácticas en realidad está también señalando estándares emergentes (y a veces consolidados) sobre la actividad de inteligencia en un Estado respetuoso de derechos humanos por cuanto se trata de sistematizar las prácticas estatales que mejor armonizan y promueven los derechos humanos en las labores de inteligencia. Finalmente, la Corte IDH, en el citado caso CAJAR, igualmente considera que estas buenas prácticas representan un documento relevante.

En tercer término, encontramos los llamados "Principios Tshwane" o, según su denominación completa, los "Principios globales sobre seguridad nacional y el derecho a la información"(13). Estos principios tampoco son en sí mismos vinculantes, pero representan igualmente una fuente doctrinaria autorizada relevante e importante: luego de una amplísima consulta, en que participaron más de 500 académicos de más de 70 países, fueron adoptados en junio de 2013 en Tshwane, en Sudáfrica, con la participación de 22 importantes centros de investigación y organizaciones de derechos humanos, como la Comisión Internacional de Juristas, Amnistía Internacional o la Universidad de Budapest.

El proceso contó con la participación y apoyo de al menos cuatro relatores especiales en derechos humanos, a saber, los entonces relatores de Naciones Unidas sobre libertad de expresión y sobre contraterrorismo y derechos humanos, la relatora interamericana sobre libertad de expresión y el relator de expresión y el relator sobre libertad de expresión de la Comisión Africana de Derechos Humanos y Derechos de los Pueblos. Por eso estos "Principios Tshwane" fueron reconocidos por organizaciones internacionales, como la Asamblea Parlamentaria del Consejo de Europa, y han sido considerados una sistematización apropiada de los estándares internacionales sobre derecho a la información y seguridad nacional, para muchos temas, como la protección de los llamados *whistle-blowers* o denunciantes (Colvin, 2018). Igualmente, la

(11) Esos principios han sido publicados en múltiples oportunidades y sitios. Para sus siguientes menciones, utilizo el texto publicado como anexo por el entonces Relator de Libertad de Expresión, Abid Hussain, en su informe de 1996 a la entonces Comisión de Derechos Humanos de Naciones Unidas con código E/CN.4/1996/39.

(12) Para un balance de estos principios, *véase* "The Johannesburg Principles: Overview and implementation" de Toby Mendel (2003).

(13) El texto de estos principios puede ser consultado en "The Global Principles on National Security and the Right to Information (Tshwane Principles)" de Open Society Foundations (2013).

Corte IDH, en el citado caso CAJAR, se refiere reiteradamente a estos principios.

En cuarto término, en 2014, por solicitud de la Asamblea General, la Alta Comisionada de Naciones Unidas para los Derechos Humanos (en adelante, ACNUDH) presentó ante el Consejo de Derechos Humanos un informe sobre las implicaciones para el derecho a la privacidad de la revolución digital, que permite a distintos actores, incluidas las autoridades de inteligencia, recoger, sistematizar y conservar masivamente datos personales. Este informe es relevante, pues representa una sistematización doctrinaria de la más alta funcionaria de Naciones Unidas en derechos humanos sobre los principios de derechos humanos y las buenas prácticas en este campo.

En quinto término, encontramos los desarrollos que sobre el tema ha tenido el TEDH, el cual en numerosas sentencias ha debido enfrentar las tensiones entre el derecho a la protección de la vida privada, las actividades de inteligencia y las competencias de las autoridades, desde el clásico caso Klass vs. Alemania de 1979 hasta la importantísima y reciente sentencia Big Brother Watch y otros contra Reino Unido, decidida en 2021 por la Grand Chamber, pasando por otros casos igualmente importantes, como los siguientes: Kennedy vs. Reino Unido, decidido en 2010; Roman Zakharov vs. Russia, decidido en 2015; Szabó y Vissy vs. Hungría, decidido en 2016 o Breyer vs. Alemania, decidido en 2020.

Igualmente, el TEDH ha tenido que abordar, en un número menor de casos, pero con decisiones relevantes, desarrollos específicos sobre como armonizar el derecho de acceso a la información, incluyendo acceso a datos personales, y las actividades policiales y de inteligencia, como los siguientes: Leander vs. Suecia, decidido en 1987; Segerstedt-Wiberg y otros vs. Suecia, decidido en 2006; M.K. vs. France decidido en 2013 o Catt vs. Reino Unido decidido en 2019[(14)]. Aunque obviamente la jurisprudencia del TEDH no es formalmente una fuente de derecho directa para América Latina, muchos de nuestros tribunales constitucionales y la propia Corte IDH la han tenido en cuenta por cuanto han considerado, con buenas razones, que la fina jurisprudencia del TEDH es una doctrina persuasiva para el desarrollo de los estándares interamericanos de derechos humanos.

Finalmente, y de particular importancia para nuestra región, encontramos la jurisprudencia de la Corte IDH, no solo las sentencias ya citadas sobre el derecho de acceso a la información (casos Claude Reyes vs. Chile y Gomes Lund y otros (guerrilha do Araguaia) vs. Brasil) sino también aquellas otras sentencias en que se aborda el marco de derechos humanos de las operaciones de inteligencia. En algunas de ellas, como las sentencias Myrna Mack Chang vs Guatemala del 25 de noviembre de 2003 o Hermanos Landaeta Mejías y otros vs Venezuela del 27 de agosto de 2014, ese abordaje es breve y tangencial. Por ello, es tan importante la reciente sentencia CAJAR por cuanto, en ella, la Corte IDH desarrolla, por primera vez, en los párrafos 516 a 608, un estudio sistemático y apropiado del tema. Esta sentencia se vuelve entonces un referente ineludible en América Latina para esos debates sobre operaciones de inteligencia y derechos humanos en general y derechos a la intimidad y al *habeas data* en particular.

6. Principios y estándares para armonizar los derechos a la privacidad y a la honra, el habeas data y las actividades de inteligencia

Con base esencialmente en las fuentes jurídicas señaladas en el aparte anterior, en este punto intento sistematizar los principios de derechos humanos que se han ido consolidando en el derecho internacional y en el derecho comparado para armonizar las actividades de inteligencia con la protección de la privacidad y los derechos de acceso a la información y al *habeas data*. He clasificado estos principios en dos grupos, por razones de claridad. El primer grupo, que denomino las "garantías formales y sustantivas", está constituido por unos principios que no son particularmente novedosos, aunque sean de enorme importancia: representan esencialmente la aplicación de los criterios generales sobre limitaciones admisibles de un derecho humano -legalidad, objetivo legítimo y proporcionalidad- al campo de las restricciones posibles a los derechos de *habeas data* y acceso a la información frente a actividades y archivos de inteligencia. El segundo grupo, que denomino las "garantías institucionales", es específico e implica ciertas novedades pues deriva de las particularidades que tienen las labores de

(14) Sobre la evolución del tema en la jurisprudencia del TEDH, *véase* "The approach of the Strasbourg Court: Article 8 ECHR and interception of communicatios" de Ni Loidean (2025).

inteligencia en una sociedad democrática, las cuales exigen garantías suplementarias específicas.

6.1. Las garantías formales y sustantivas clásicas: legalidad, objetivo legítimo, y proporcionalidad

Como lo presenté anteriormente, el derecho internacional reconoce el derecho de acceso a la información y el *habeas data*, por lo cual, en principio, toda persona tiene derecho a acceder a los archivos en poder de las autoridades, incluidos, *prima facie*, los archivos de inteligencia. Y con mayor fuerza, toda persona, conforme al *habeas data*, tiene derecho a acceder a sus datos personales contenidos en archivos de inteligencia y, si es el caso, solicitar su corrección o supresión. Una negativa de las autoridades a entregar esas informaciones representa entonces una restricción a esos derechos o, usando el lenguaje de ciertas instancias de derechos humanos, una interferencia en esos derechos.

Por ello, para que esa restricción o esa interferencia sea legítima debe reunir los requisitos comunes a cualquier limitación de un derecho humano, tomando en cuenta, obviamente, las particularidades de las actividades de inteligencia. Por eso todas las seis fuentes jurídicas coinciden en señalar, en una forma u otra, que esas restricciones al *habeas data* o al derecho de acceso a datos personales en archivos de inteligencia deben cumplir con los tres requisitos propios de cualquier limitación a un derecho: (i) legalidad, (ii) objetivo legítimo o legitimidad, y (iii) proporcionalidad. Procedo entonces a desarrollar esos tres requisitos, enfatizando aquellos elementos peculiares al *habeas data* frente a actividades de inteligencia, lo cual permitirá inferir ciertos estándares suplementarios relativos a la relación entre el derecho de acceso a la información y los archivos de inteligencia.

6.1.1. Legalidad de la reserva

La legalidad implica que la restricción esté "expresamente establecida en la ley", como lo dicen el artículo 13 de la CADH y en forma semejante el artículo 19 del PIDCP puesto que se trata de una restricción de la libertad de expresión, en su componente de derecho de acceso a la información y vinculado a los derechos a la privacidad y a la honra, esto es, al derecho al *habeas data*. Esta garantía implica no solo que esas restricciones estén previstas formalmente en una ley, sino que, además, en el lenguaje del TEDH, esa ley debe tener ciertas "cualidades": obviamente deber ser pública pero igualmente tiene que ser clara y precisa, de suerte que los ciudadanos puedan prever con claridad los alcances de sus derechos y de las competencias de las autoridades de inteligencia.

La ley debe entonces ser accesible para la persona afectada y sus efectos deben ser previsibles, como lo indica el citado fallo Rotaru vs. Rumania del TEDH, decidido en 2000, en su párrafo 52. Y esto vale, tanto en (i) relación con las actividades de inteligencia que puedan afectar la privacidad, las cuales deben estar determinadas en la ley, como sobre los (ii) documentos que tienen reserva por estar vinculados a ciertas actividades de inteligencia. Por eso, en ciertos casos, el TEDH ha concluido que ciertas actividades de vigilancia realizadas por instancias de inteligencia no respetaban el principio de legalidad pues la ley no era suficientemente precisa.

En esa línea, es importante la sentencia de Liberty y otros vs. Reino Unido, decidida en 2008, en que el TEDH concluyó que el derecho a la privacidad de tres organizaciones de derechos humanos había sido violado, a las cuales, entre 1990 y 1997, les fueron interceptados sus teléfonos y correos electrónicos por el Ministerio de Defensa, en desarrollo de una operación de monitoreo masivo de comunicaciones entre Dublín y Londres. El TEDH consideró que la ley británica no era suficientemente clara para proveer protección adecuada contra el abuso de poder ya que daba demasiada discreción a las autoridades para interceptar y examinar las comunicaciones. En particular, la ley no establecía criterios y procedimientos para determinar cuáles informaciones provenientes de ese monitoreo masivo podían ser examinadas, archivadas y compartidas a ciertas agencias estatales o cuando esas informaciones debían ser destruidas.

En otros casos, el TEDH ha examinado si la ley prevé con suficiente claridad cuáles son los documentos sometidos a reserva por razones de seguridad nacional o seguridad pública. Al respecto, el caso Leander vs. Suecia, decidido en 1987. En los párrafos 52 a 57, el TEDH encontró que la ley sueca era suficientemente accesible a los ciudadanos y previsible sobre la información reservada y la actividad desplegada por las autoridades de inteligencia, por lo cual era compatible con la CEDH.

Conforme a lo anterior, la legalidad implica una definición legal adecuada y

(15) La práctica Sheinin 2 señala. "Los mandatos de los servicios de inteligencia deben estar definidos con rigor y precisión en una ley a la que el público tenga acceso. Los mandatos deben limitarse estrictamente a proteger los intereses legítimos de la seguridad nacional, definidos en leyes o políticas de seguridad nacional a las que el público tenga acceso y a identificar las amenazas a

detallada de la estructura y operación de los servicios de inteligencia, como lo señalan las "buenas prácticas Scheinin" No. 2[15] y No. 4[16], por lo cual cualquier delegación de esas regulaciones en reglamentos debe ser cuidadosa y resulta inadmisible en reglamentos secretos. Por su parte, como señala la práctica 21[17], debe estar igualmente regulado legalmente los elementos esenciales de cuál información puede ser recolectada, sistematizada y usada por esos servicios de inteligencia.

Por su parte la Corte IDH, en el párrafo 50 de la citada sentencia del caso CAJAR, distingue acertadamente entre la reserva que caracteriza la labor de inteligencia y la necesidad de publicidad de su marco normativo. Y por ello la Corte IDH enfatiza que la ley que regula las actividades de inteligencia debe ser "accesible para el público" por cuanto:

> A diferencia de las actividades de inteligencia propiamente dichas, el marco legal que las autoriza y regula nunca puede ser de carácter reservado, permitiendo así que las personas conozcan las facultades del Estado en este ámbito y, a partir de ello, estén en capacidad de prever que eventualmente tales actividades podrían incidir en su esfera propia de derechos (2023).

6.1.2. Legitimidad del objetivo de la reserva

La legitimidad de la reserva de información tiene que ver con la legitimidad del objetivo perseguido por las actividades de inteligencia, las cuales, conforme al artículo 13 de la CADH y 19 del PIDCP solo pueden ser la seguridad nacional, el orden público, la moral y salud públicas y la protección de otros derechos humanos. Ahora bien, por la naturaleza de las actividades de inteligencia, los objetivos legítimos usualmente señalados y que son válidos conforme al derecho internacional son el orden público y la seguridad nacional, aunque no puede excluirse que también en ciertos casos pueda invocarse la salud pública y la protección de otros derechos humanos.

En este aspecto del objetivo perseguido aparentemente no parece haber mayores controversias ni necesidad de desarrollo de estándares, pero no es así por las siguientes dos razones.

Primero, es necesario que la ley fije con relativa precisión qué se entiende por seguridad nacional u orden público y cuáles componentes de esos conceptos justifican labores de monitoreo o reserva de documentos. Como bien dice el principio 12 de los Principios de Johannesburgo, la excepción de seguridad nacional para acceso a documentos públicos debe estar especificada, por lo cual un Estado no puede negar acceso a toda la información relativa a la seguridad nacional, sino que "debe establecer legalmente solamente aquellas categorías limitadas y específicas de información que ese necesario reservar para proteger un interés legítimo de seguridad nacional". Los principios 9 y 10 de los principios Tshwane van en la misma dirección e incluso especifican más detalladamente cuáles podrían ser los componentes de la seguridad nacional que justificarían una reserva documental -como podría ser la información sobre los planes actuales de defensa y las operaciones militares previstas, mientras esa información sea operacionalmente relevante- y por el contrario cuáles aspectos, aunque pudieran tener relación con la seguridad nacional, no deberían tener reserva, como sería la información relativa a cuáles son los órganos de supervisión de las actividades de inteligencia.

Segundo, al definir los objetivos legítimos de las actividades de inteligencia y que podrían justificar la reserva de documentos y de información, es necesario igualmente que la ley precise aquellos propósitos para los cuales nunca pueden ser usadas esas actividades inteligencia y que tampoco pueden justificar una reserva documental, como pueden ser la persecución política a los opositores o el perfilamiento de personas únicamente basado en sus opiniones, sin

---

la seguridad nacional que los servicios de inteligencia tienen que combatir. Si el terrorismo figura entre estas amenazas, deberá definirse con rigor y precisión".

(16) La Práctica Sheinin 4 establece. "Todos los servicios de inteligencia están constituidos en virtud de leyes a las que el público tiene acceso y que respetan las disposiciones de la Constitución y la normativa internacional de derechos humanos, y funcionan con arreglo a esas leyes. Los servicios de inteligencia solo pueden emprender actividades, o recibir instrucciones de emprenderlas, que estén contempladas en la legislación nacional y sean conformes con ella. La aplicación de reglamentos subsidiarios está estrictamente limitada y sujeta a las disposiciones de leyes a las que sí tiene acceso el público. Los reglamentos que no se pongan en conocimiento del público no sirven de base para ninguna actividad que coarte los derechos humanos".

(17) La Práctica Sheinin 21 señala: "La legislación nacional define los tipos de medidas de recopilación que pueden emplear los servicios de inteligencia, los objetivos permisibles de la recopilación de información; las clases de personas y actividades respecto de las cuales puede recopilarse información; el grado de sospecha que justifica la recopilación de información; los plazos dentro de las cuales puede recopilarse la información; y los procedimientos para actualizar, supervisar y examinar las medidas de recopilación de información".

que exista ningún otro hecho que justifica la vigilancia, o que se prevean formas discriminatorias de labores de inteligencia. O que la labor de inteligencia y la información reservada en archivos recaigan sobre ámbitos que tienen una protección especial, como las conversaciones entre los clientes y sus abogados o la labor de los periodistas, como lo destaca con vigor la sentencia CAJAR en los párrafos 555 a 561. En particular, en ese último párrafo, la Corte IDH destaca que existe una "protección reforzada" de la función de los periodistas y abogados, por lo cual:

> Cualquier operación de inteligencia en este ámbito únicamente podrá realizarse con autorización judicial previa, correspondiendo al juez competente decidir acerca de (i) la presencia de indicios sobre la práctica de actos ilícitos, y (ii) la proporcionalidad de la medida dispuesta en el caso concreto (2023, párr. 561).

Otro punto muy relevante para nuestra región es la exclusión de reserva sobre graves violaciones a los derechos humanos y al derecho internacional humanitario, en especial si dicha reserva afecta el derecho a la verdad de las víctimas y sus familiares o representa un obstáculo para la rendición de cuentas de los victimarios. Así lo señala el Principio Tshwane 10, en perfecta armonía con lo desarrollado por la Corte IDH en la sentencia Gomes Lund y otros vs. Brasil.

6.1.3. Proporcionalidad de la reserva

El análisis de proporcionalidad debe aplicarse en general a todas las labores de inteligencia, como bien lo señala el párrafo 537 de la citada sentencia CAJAR. Y en particular ese mismo test de proporcionalidad debe aplicarse a cualquier reserva de información -o a cualquier posible interferencia de las actividades de inteligencia en la privacidad- por razones de seguridad nacional u orden público. Esto implica que debe tratarse de reservas o interferencias en la privacidad necesarias en una sociedad democrática para lograr esa protección del orden público y de la seguridad nacional.

Por ello, las reservas deben respetar el principio de proporcionalidad, en el triple sentido reconocido ampliamente por la doctrina. Debe entonces tratarse de medidas (i) adecuadas para alcanzar esos propósitos y, además, (ii) necesarias, en el sentido de que no existan otras medidas igualmente eficaces para lograr esos propósitos pero que sean menos restrictivas al habeas data y al derecho de acceder a la información. Y además la reserva documental debe ser (iii) proporcionada en estricto sentido, esto es, la afectación del *habeas data* o del derecho de acceso a documentos debido a la reserva debe aparecer proporcionada al daño a la seguridad nacional o al orden público que se pretende prevenir[18]. Esto significa en particular que la información que sería revelada implica, como lo señala el Principio Tshwane 3, una afectación a la seguridad concreta identificable que tiene mayor peso que el impacto sobre el acceso a la información que implica esa reserva; y en todo caso debe respetarse la esencia del derecho a la información.

6.2. Consideraciones especiales por la naturaleza reservada de las actividades de inteligencia

Estos tres requisitos generales para que una reserva de archivos de inteligencia sea compatible con el derecho internacional de los derechos humanos adquieren unas connotaciones específicas frente a archivos de inteligencia, dada la propia naturaleza de las actividades de inteligencia, a saber, que son realizadas usualmente en secreto y sin el consentimiento de los ciudadanos eventualmente afectados por esa vigilancia. Brevemente señalo algunas de esas implicaciones, sin pretensión de exhaustividad, por cuanto tales implicaciones son tratadas con suficiente detalle en las seis fuentes mencionadas en el punto anterior.

Primero, la reserva legal es más estricta. La Corte IDH, en la citada sentencia CAJAR, en el párrafo 577 señala que, debido a que los organismos de inteligencia pueden recopilar y mantener datos sobre las personas, sin su consentimiento, la ley debe prever "con especificidad, las facultades de los organismos de inteligencia para la recopilación de datos personales, así como para implementar y mantener archivos que incluyan tales datos" (2023). Y esa ley debe entonces regular con la mayor precisión posible aspectos como los siguientes: (i) los motivos que habilitan la existencia de esos archivos de datos personales por los organismos de inteligencia; (ii) las clases y tipos de datos de carácter personal que pueden ser recolectados y conservados en esos archivos, y (iii) "los parámetros aplicables para la utilización, conservación, verificación, rectificación, eliminación o revelación de tales datos".

Segundo, la Corte IDH, en el párrafo 540 de la citada sentencia CAJAR, señala que a fin de facilitar el control a las operaciones

(18) Sobre los principios de necesidad y proporcionalidad en estricto sentido aplicados a las actividades de inteligencia en general y a la reserva de documentos, *véase* el principio 1 de los Principios de Johannesburgo y los párrafos 25 a 27 del Informe ACNUDH.

de inteligencia y reducir los riesgos de abusos, es necesaria "la formalización, por medio de procesos numerados, de las distintas actividades de inteligencia emprendidas, con el debido registro de todas sus etapas, incluido el historial de registros de acceso a sistemas electrónicos" (2023). Y en particular, frente al procesamiento de datos personales, debe existir lo siguiente:

> (...) Un registro que (i) identifique a los responsables de dicho procesamiento; (ii) los propósitos para el procesamiento de la información recopilada, indicando el origen y categoría de los datos; (iii) la base jurídica de las operaciones realizadas; (iv) los plazos de conservación, y (v) las técnicas utilizadas para su tratamiento (2023, p. 162)

Tercero, la reserva de los archivos de inteligencia no puede ser perpetua, sino que debe ser temporal, por cuando las razones que podían justificar una restricción de acceso en un determinado momento se van debilitando con el paso del tiempo, al punto de hacerla ilegítima posteriormente por desproporcionada(19).

Cuarto, debe existir un mecanismo de depuración y desclasificación de los documentos reservados, que permita que aquellos cuya reserva ya no esté justificada pasen a ser accesibles al público en general o a las autoridades y personas interesadas en particular, según los distintos niveles de reserva previstos en el ordenamiento jurídico. O que esa información sea eliminada de los archivos de inteligencia, al haber perdido toda relevancia(20).

Además, quinto, como lo señala la buena práctica Scheinin 24(21), este mecanismo de depuración no solo debe hacer accesibles los documentos cuya reserva perdió justificación con el paso del tiempo, sino que debe igualmente tener la capacidad de detectar cuál información, incluso reciente, no debe hacer parte de esos archivos reservados de inteligencia y debe ser eliminada, por ejemplo, por tratarse de información discriminatoria o que no tiene ninguna relevancia para la seguridad pública. O que, pudiendo hacer parte de esos archivos, no debe tener reserva y ser accesible al público por cuanto un análisis de proporcionalidad muestra que no estaba justificada su reserva.

Esto lleva, sexto, a un punto sobre el cual los estándares están aún en consolidación pero que me parece justificado, conforme a los principios de derechos humanos: son aquellos casos en que los Estados tendrían no solo el deber de levantar la reserva, sino que adquieren un deber proactivo de divulgación, al menos a ciertas personas afectadas. Se trata de aquellos eventos en que el Estado constata que hubo una ilegalidad que afectó en forma sensible un derecho ciudadano. En esos eventos, no solo la información ya no debe tener reserva, sino que considero que, siguiendo lo señalado por los principios 10 y 21 de los Principios Tshwane, es deber del Estado, como expresión de su obligación de garantizar los derechos humanos y reparar las violaciones ocurridas, informar proactivamente al ciudadano de esos hechos, para que éste pueda tomar las medidas apropiadas para salvaguardar sus derechos y eventualmente solicitar la correspondiente reparación.

Una pregunta obvia surge del anterior análisis. Dada la reserva inherente a las actividades de inteligencia: ¿cómo pueden y deben operar esos mecanismos de depuración y supervisión de la información reservada en actividades de inteligencia, a fin de verificar si la información recolectada es conforme a los estándares de derechos humanos y si la reserva está justificada? Esta pregunta es trascendental e implica una particularidad de la protección del *habeas data* y del derecho de acceso a archivos de inteligencia frente a la operatividad de esos derechos en otros campos, por lo cual conviene tratarlo en forma específica en el siguiente punto.

6.3. Las garantías institucionales: necesidad de órganos independientes de supervisión y autorización, complementados con la posibilidad de un recurso judicial efectivo

La doctrina usual para la protección de un derecho humano es que éste debe contar con un recurso judicial que la persona afectada pueda utilizar en caso de una violación o amenaza a su derecho, como lo señala el

(19) Por ejemplo, *véase* el Principio Tshwane 16, el cual señala que esa reserva solo puede mantenerse mientras sea necesaria y no puede ser perpetua.

(20) Para mayor profundización, *véase* el Principio Tshwane 17 sobre los procedimientos de depuración y desclasificación de los archivos de inteligencia.

(21) Al respecto, dice la Práctica Sheinin 24: "Los servicios de inteligencia llevan a cabo evaluaciones regulares de la pertinencia y la exactitud de los datos personales en su poder. Estos servicios están legalmente obligados a suprimir o actualizar cualquier información que se haya determinado que no es exacta o que ya no sea pertinente para su mandato, la labor de las instituciones de supervisión o posibles actuaciones judiciales" (2010, p. 24).

artículo 25 de la CADH. Y esto es así también frente al derecho de acceso a la información y al *habeas data*, por lo cual las personas deben contar con la posibilidad última de recurrir ante un juez para que las ampare en su derecho.

Además, fuera de esa posibilidad de acción judicial posterior, muchas de las operaciones de inteligencia requieren, a fin de prevenir abusos, una autorización judicial previa. Por eso, en los párrafos 542 y ss. de la citada sentencia CAJAR, la Corte IDH especifica, con bastante detalle, las actividades de inteligencia que, según ese tribunal, necesitan una autorización judicial previa. Esos párrafos son importantes pues la Corte IDH no solo se refiere a situaciones clásicas que tienen reserva judicial, como la interceptación de comunicaciones de una persona, sino que también plantea que esa autorización judicial es necesaria para otras operaciones, como aquellas "que impliquen el acceso a bases de datos y sistemas de información no públicos que almacenen y procesen datos personales, el rastreo de usuarios en la red informática o la localización de dispositivos electrónicos" (Párrafo 553).

Sin embargo, frente a actividades de inteligencia, la autorización judicial previa o el recurso judicial activado por el ciudadano, aunque necesarios, resultan insuficientes, por una obvia razón: esas actividades son usualmente secretas y sus archivos están sujetos a reservas de distinta intensidad, por lo cual le resulta al ciudadano muy difícil, cuando no imposible, enterarse si está sujeto a una vigilancia violatoria de su privacidad o si los servicios de inteligencia mantienen en sus archivos y comparten con otras autoridades información personal que no deberían estar en esos archivos, por ser irrelevante, inexacta, discriminatoria, obtenida ilegalmente, etc. Por ejemplo, en Colombia, especialmente durante los gobiernos de Álvaro Uribe Vélez, el Departamento Administrativo de Seguridad, DAS, sometió ilegalmente a vigilancia y archivó información de personas que nunca supieron de esos crímenes, como periodistas o jueces, incluyendo a integrantes del sistema interamericano de derechos humanos.

Por lo anterior, una de las conclusiones esenciales a las que llegan las fuentes jurídicas citadas en el anterior punto es que frente a las eventuales violaciones de derechos humanos por los servicios de inteligencia no es suficiente la previsión de un recurso judicial eventual por parte de la persona afectada, aunque ese recurso deba en todo caso existir. La conclusión es que la única forma de lograr que los servicios de inteligencia cumplan con sus importantes funciones y puedan operar en reserva, pero sin amenazar o violar los derechos humanos, es que existan una o varias instituciones, que sean independientes de esos servicios, pero que ejerzan un monitoreo permanente sobre sus actividades y tengan la posibilidad de tomar ciertas decisiones frente a esas labores.

Así lo prevén el principio de Johannesburgo 14, los principios Tshwane 26 y en especial 31 a 36 y las buenas prácticas Scheinin 6, 7, 8, 22, 25 y 26. Igualmente así lo señala el informe de la ACNUDH en los párrafos 37, 38 y 50 y se desprende claramente de la jurisprudencia sobre el tema del TEDH. Igualmente, el párrafo 564 de la sentencia CAJAR enfatiza la importancia de esas instituciones independientes de control al indicar que:

> En cuanto a la supervisión de las actividades de inteligencia, se hace necesario que el marco jurídico establezca, sin perjuicio del control judicial sobre medidas o acciones específicas en situaciones concretas, una institución civil independiente de los servicios de inteligencia y del Poder Ejecutivo, de naturaleza parlamentaria, administrativa o jurisdiccional, la cual, además de contar con los conocimientos técnicos sobre la materia, debe estar dotada de las facultades para ejercer sus funciones, incluido el acceso directo y completo a la información y los datos indispensables para cumplir su cometido. El mandato de esta institución civil de supervisión debe abarcar la fiscalización en torno a los siguientes aspectos: (a) el acatamiento, por parte de los servicios de inteligencia, de las disposiciones legales que rigen su actuación y de los instrumentos sobre derechos humanos; (b) la eficiencia y eficacia de sus actividades, evaluando su rendimiento; (c) su situación financiera y presupuestaria, y la administración de sus fondos, y (d) sus métodos y prácticas administrativas (2023, p. 170).

La razón de la necesidad de esa o esas instituciones independientes de monitoreo, control y autorización frente a los servicios de inteligencia es que es la única forma de que esos servicios puedan operar en secreto, pero no abusen de sus poderes, por cuanto están sometidos a instituciones independientes de control, que tendrían el deber de mantener la reserva para no afectar la seguridad nacional, pero podrían monitorear y corregir los eventuales desvíos de los servicios de inteligencia.

Esas instituciones deben estar reguladas por la ley y deben, todas, o al menos alguna de ellas, ser civiles, independientes del gobierno y de los propios servicios de inteligencia, como bien lo señala la buena práctica Scheinin 6, que por su importancia transcribo literalmente:

> Los servicios de inteligencia están supervisados por un conjunto de instituciones de supervisión internas, ejecutivas, parlamentarias, judiciales

> y especializadas, cuyos mandatos y facultades se basan en leyes a las que el público tiene acceso. Un sistema efectivo de supervisión de los servicios de inteligencia incluye por lo menos una institución civil independiente de los servicios de inteligencia y del poder ejecutivo. El mandato combinado de las instituciones de supervisión abarca todos los aspectos de la labor de los servicios de inteligencia, con inclusión de su observancia de la ley, la eficacia y eficiencia de sus actividades, su situación financiera y sus prácticas administrativas (2010, p. 8).

Esas instituciones de monitoreo y autorización frente a las labores de inteligencia cumplen diversos propósitos, pero al menos los siguientes cuatro que son de particular relevancia.

a) Primero, un monitoreo general de los servicios de inteligencia, con el fin de evaluar su eficacia y legitimidad y corregir sus disfunciones; en muchas ocasiones, ese monitoreo es realizado por un órgano externo, usualmente parlamentario.
b) Segundo, alguna o algunas de esas instituciones deberían autorizar ciertas labores de vigilancia, que no requieran autorización judicial pero que implican una afectación de la privacidad importante, por lo cual no deberían ser tomadas por los propios agentes de inteligencia o sus superiores jerárquicos por el obvio conflicto de interés, como podría ser un perfilamiento o seguimiento de alguna persona, sin llegar a interceptar sus comunicaciones puesto que esto último obviamente requiere autorización judicial.
c) Tercero, alguna o algunas de esas instituciones debe tener la tarea de resolver las solicitudes de acceso a la información, pudiendo entonces revisar los archivos para determinar si la información existe o no y si la reserva está justificada o no.
d) Cuarto, alguna o algunas de esas instituciones debería tener la tarea de realizar o supervisar las labores permanentes de depuración de los archivos de inteligencia.

No existe un modelo único de cómo organizar esa o esas instituciones de monitoreo, control y autorización. Como lo muestra el sistemático informe de buenas prácticas Scheinin, algunos Estados tienen a prever y combinar varias instituciones, incluso de diversa naturaleza, para realizar esas labores, mientras que otros Estados optan por un diseño institucional más unificado.

Considero que es difícil establecer, en términos de política pública, cual diseño es el más apropiado, no solo por cuanto no existen, o al menos no conozco, evaluaciones sistemáticas al respecto sino, además, porque es posible que el contexto nacional sea decisivo y que entonces un diseño muy apropiado en un país resulte disfuncional en otro. Lo importante es que se trate de una o varias instituciones independientes y que cuenten con las competencias jurídicas y los recursos económicos y burocráticos para desarrollar adecuadamente al menos las cuatro funciones mencionadas anteriormente.

El caso Segerstedt-Wiberg y otros vs. Suecia, decidido en 2006 por el TEDP, muestra que la existencia de esas instituciones de monitoreo, junto con los criterios formales y sustantivos señalados en el punto 4.1. de este artículo, permiten una evaluación concreta de la adecuación o no a los estándares de derechos humanos de la decisión de reservar o no cierta información de inteligencia. En ese caso, cinco personas buscan acceder a los registros de inteligencia policial, que les fueron negados. Luego de examinar que la regulación legal sueca respetaba el principio de legalidad, pues era suficientemente precisa y previsible, y que el objetivo perseguido era legítimo, que era proteger la seguridad pública, el TEDH encuentra que, sin embargo, en relación a ciertos peticionarios, hubo violación del derecho a la privacidad porque la policía tenía información que era desproporcionada, a saber, que esa persona había defendido la resistencia violenta contra la policía tres décadas antes. El TEDH encontró que esa información pudo ser relevante en su momento pero que mantenerla después de tres décadas implicaba una invasión desproporcionada a la privacidad del peticionario. Por el contrario, el TEDH encontró que no violaba el derecho a la privacidad que la policía hubiera negado el acceso general de los peticionarios a todo el expediente policial, por cuanto esa negativa era legal, perseguía un objetivo legítimo y, sobre todo para nuestro análisis, Suecia contaba con suficientes garantías e instituciones independientes de control que le permitían al TEDH concluir que no había arbitrariedad en esa negativa.

El TEDH hizo referencia al menos a cuatro instancias de control de la labor de inteligencia policial, con distintos grados de independencia y atribuciones: (i) la junta de registros (Records Board), formada por ocho integrantes, incluidos al menos dos con experiencia judicial, que monitorea si la información archivada respeta los criterios legales y es procedente o no levantar su reserva; (ii) la junta de inspección de datos (Data Inspection Board), que es también independiente y recibe y tramita quejas individuales relativas a posible almacenamiento indebido de datos privados; (iii) el Ombudsman, que es independiente

y realiza un monitoreo general de la actividad policial, con facultades para realizar inspecciones para evaluar la legalidad de sus actuaciones; y (iv) el llamado *Chancellor of Justice*, que puede tramitar quejas relativas a comportamientos policiales indebidos y puede incluso ordenar compensaciones, en caso de que haya habido ilegalidades. Y en todo caso, algunas de las decisiones de esas instancias independientes podían ser cuestionadas ante jueces independientes.

Como vemos, la presencia o no de esas instituciones independientes de monitoreo y control es esencial para determinar si una negativa a la solicitud de acceso a un archivo de inteligencia viola o no el habeas data o el derecho de acceso a la información. Con todo, en este caso, el TEDH encontró que, a pesar de su buen desarrollo institucional, las facultades de esos órganos independientes suecos eran en ciertos aspectos insuficientes. Por ejemplo, que la Junta de Registros carecía de la facultad la eliminación o rectificación de información indebida en los archivos policiales. Por eso el TEDH consideró que en todo caso a los peticionarios les fue violado el derecho a un recurso efectivo frente a eventuales violaciones a su privacidad.

7. Conclusiones y reflexiones finales

Considero que este artículo tiene tres aportes importantes al derecho de los derechos humanos. Primero, contribuye a fundamentar el reconocimiento en el derecho internacional y en particular en el sistema interamericano del *habeas data*, en mi terminología, o del derecho a la autodeterminación informativa, en el lenguaje de la Corte IDH y de otros autores, como un derecho humano autónomo, aunque profundamente ligado a otros derechos fundamentales: intimidad, buen nombre y acceso a la información. No es un tema menor dada la importancia que tiene el *habeas data* en el mundo digital en que vivimos.

Segundo, el artículo sistematiza, con base en las fuentes jurídicas hoy más relevantes, los principales estándares de derechos humanos aplicables a las labores de inteligencia, a fin de que estas sean eficaces, pero no violen los derechos humanos, en especial los derechos a la intimidad, al buen nombre y al *habeas data.* Este esfuerzo de sistematización no es totalmente original, pues varios de los documentos citados en este artículo, como las Prácticas Scheinin o los Principios Tshwane, pretenden una sistematización semejante; sin embargo, este artículo tiene la virtud de articular todos esos documentos de *soft law* y tomar en cuenta desarrollos más recientes no totalmente sistematizados previamente, en especial la sentencia CAJAR de la Corte IDH y ciertas decisiones recientes del TEDH. En ese sentido es una sistematización más actualizada y tal vez más relevante para América Latina

Tercero, el artículo tiene la virtud de resaltar un punto trascendental, que muchas veces no es enfatizado suficientemente en las discusiones sobre la regulación de las labores de inteligencia: la importancia de que, además de los recursos judiciales, existan instituciones civiles independientes del gobierno y de las autoridades de inteligencia y que, manteniendo la reserva necesaria, ejerzan un monitoreo y control permanentes y eficaces sobre dichas autoridades. Todo indica que sin la presencia de esa o esas instituciones, pues los diseños nacionales pueden ser diversos, es imposible garantizar que las democracias tengan servicios de inteligencia eficaces y al mismo tiempo respetuosos de los derechos humanos.

Creo que esos aportes son particularmente importantes para América Latina por cuanto nuestros países enfrentan formas intensas de violencia y crimen organizado que amenazan los derechos ciudadanos y ponen en peligro el orden público. Esta situación ha llevado al desespero a ciertos sectores de la ciudadanía, que apoyan entonces soluciones extremas autoritarias, tipo Bukele, que ha implicado la privación de la libertad y en condiciones indignas, sin controles judiciales adecuados, de miles de personas. Sin embargo, esas opciones no solo son inaceptables democráticamente, pues implican violaciones masivas a los derechos humanos, sino que, además, en el mediano plazo, son contraproducentes por cuanto esos gobernantes, desprovistos de controles, terminan involucrados en graves abusos y formas de corrupción. El caso de Fujimori en el Perú es ilustrativo de esos terribles riesgos.

Necesitamos entonces Estados eficaces que sean capaces de hacer frente al crimen organizado y a los desafíos a la seguridad pues nuestra región no está poblada de ángeles, por recordar la referencia a Madison que encabeza este artículo. No podemos entonces, quienes trabajamos en derechos humanos, pensar únicamente en cuáles son las restricciones normativas que tienen las autoridades, sino que debemos también reflexionar sobre como incrementamos las capacidades de nuestras instituciones. Pero nuestros gobernantes tampoco son ángeles, por lo cual no podemos apostarle

a que la solución sea un Leviatán despótico y sin controles pues tenemos que aprender de la terrible experiencia de las dictaduras y gobiernos autoritarios en nuestra región.

En este contexto, el libro relativamente reciente de los premios Nóbel de economía del 2024, Acemoglu y Robinson (2019), que lleva por título sugestivo "el pasillo estrecho", resulta relevante. Su tesis esencial, sustentada en amplias referencias históricas, es que la libertad y la seguridad solo se logran por aquellas sociedades que transitan ese camino estrecho, que consiste en construir Estados robustos, que sean entonces capaces de someter a una sociedad que no está compuesta de ángeles, pero siempre y cuando esos Estados estén acompañados de controles y de una sociedad civil fuerte y vigilante, para evitar los abusos de los gobernantes, que tampoco son ángeles. Debemos entonces evitar, en la terminología de estos autores, tanto un "*Leviatán ausente*", por cuanto esos Estados ineficaces no logran el orden ni evitan la violencia, como un "*Leviatán despótico*", que abusaría de sus poderes al carecer de controles y de contrapesos en la sociedad civil. Requerimos una forma de "*Leviatán encadenado*", que es en el fondo la forma como Acemoglu y Robinson denominan lo que podría uno llamar una democracia constitucional y un Estado de derecho eficaz.

Esta reflexión es particularmente pertinente en América Latina por cuanto nuestros Estados parecen atrapados en un equilibrio perverso y una especie de trampa institucional de calidad media, como lo plantean los politólogos Mazzuca y Munck (2021). Ese equilibrio perverso consiste en que tenemos democracias muy imperfectas y débiles -con alta corrupción y clientelismo, abusos estatales, poderes regionales despóticos, etcétera-, y Estados con capacidades muy limitadas para asegurar la provisión de bienes públicos, como la seguridad, por lo cual tenemos serios problemas de violencia y criminalidad. Y esta situación persiste por cuanto existe un círculo vicioso que precisamente lleva a ese equilibrio perverso: los problemas de incapacidad estatal impiden una democracia más plena y las debilidades democráticas impiden un fortalecimiento de las capacidades estatales. Debemos entonces caminar el pasillo estrecho y superar ese equilibrio perverso, a fin de construir instituciones eficaces pero que no sean abusivas.

Es en ese contexto que creo que el esfuerzo normativo desarrollado en este artículo adquiere vigencia y pertinencia pues considero que los estándares normativos que he sistematizado son realistas: permiten estructurar servicios de inteligencia eficaces para enfrentar amenazas al orden público y a la seguridad, como el crimen organizado o el terrorismo, pero incorpora los controlados apropiados a fin de que esos organismos no incurran en abusos y violaciones de derechos humanos. Es pues un insumo para transitar ese pasillo estrecho hacia democracias más plenas, eficaces y respetuosas de la dignidad humana.

Referencias bibliográficas

Alto Comisionado de las Naciones Unidas para los Derechos Humanos (ACNUDH). (2014). *The right to privacy in the digital age*. Informe del Alto Comisionado de las Naciones Unidas para los Derechos Humanos al Consejo de Derechos Humanos. https://www.ohchr.org/sites/default/files/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf

Acemoglu, D. & Robinson, J. A. (2019). *The narrow corridor: States, societies, and the fate of liberty*. Penguin Books.

Arendt, H. (1983). *Condition de l´homme moderne*. Calman-Lévy.

Bertoni, E., Salazar, D., & Zelada, C. (2019). Artículo 13: libertad de expresión. En C., Steiner & M. C., Fuchs (Eds.), *Convención Americana de Derechos Humanos: Comentario* (2.ª ed.). Konrad Adenauer Stiftung. https://www.kas.de/documents/271408/4530743/Comentario+a+la+Convenci%C3%B3n+Americana+de+Derechos+Humanos.pdf

Bobbio, B. (1994). *El futuro de la democracia*. Fondo de Cultura Económica.

Bonham, J. & Rehg, W. (Eds.) (1997). *Deliberative Democracy. Essays on Reason and Politics*. MIT Press. https://www.viaeducacion.org/downloads/ap/pn/deliberative_democracy.pdf

Botero, C., Guzmán, F., Jaramillo, S. & Gómez, S. (2017). *El derecho a la libertad de expresión: Curso avanzado para jueces y operadores jurídicos en las Américas*. Dejusticia; Universidad de los Andes; Open Society Foundations. https://www.dejusticia.org/wp-content/uploads/2017/07/El-derecho-a-la-libertad-de-expresi%C3%B3n-PDF-FINAL-Julio-2017-1-1.pdf

Cifuentes, E. (1997). El Hábeas Data en Colombia. *Derecho PUCP*, (51), 115-144. https://doi.org/10.18800/derechopucp.199701.005

Colvin N. (2018). Whistle-Blowing as a Form of Digital Resistance. *State Crime Journal, 7*(1), 24-45. ttps://doi.org/10.13169/statecrime.7.1.0024

Habermas, J. (1995). *Between facts and norms. Contributions to a discourse theory of law and democracy*. MIT Press.

García, L. (1992). *Estudios sobre el derecho a la intimidad*. Tecnos.

Hamilton, A., Madison, A. & Jay, J. (1948). *The Federalist papers*. Basil Blackwell.

Kant, E. (1985). *La paz perpetua*. Tecnos.

Hussain, A. (1996). *Informe a la Comisión de Derechos Humanos de las Naciones Unidas*

(E/CN.4/1996/39). Naciones Unidas. https://documents-dds-ny.un.org/doc/UNDOC/GEN/G96/118/04/PDF/G9611804.pdf?OpenElement

Laffer, C. (1991). *La reconstrucción de los derechos humanos: Un diálogo con el pensamiento de Hannah Arendt*. Fondo de Cultura Económica.

Mazzuca, S. L., & Munck, G. L. (2021). *A middle-quality institutional trap: Democracy and state capacity in Latin America*. Cambridge University Press.

McDonagh, M. (2013). The right to information in international human rights law. *Human Rights Law Review, 13*(1), 25–55. https://www.corteidh.or.cr/tablas/r30698.pdf

Mendel, T. (2003). *The Johannesburg Principles: Overview and implementation*. Article 19. https://www.article19.org/data/files/pdfs/publications/jo-burg-principles-overview.pdf

Mendoza, O. (2021). El derecho de protección de datos personales en los sistemas de inteligencia artificial. *Revista IUS*, *15*(48), 179-207. https://doi.org/10.35487/rius.v15i48.2021.743

Moreno, A., & Serrano, I. (Eds.). (2021). *El derecho a la protección de datos personales en Europa y en América: Diferentes visiones para una misma realidad*. Tirant lo Blanch.

Ni Loideain, N. (2025). The approach of the Strasbourg Court: Article 8 ECHR and interception of communications. En *EU data privacy law and serious crime: Data retention and policymaking*. Oxford University Press

Nino, C. (1997). *La constitución de la democracia deliberativa.* Gedisa.

Open Society Foundations. (2013). *The Global Principles on National Security and the Right to Information (Tshwane Principles)*. https://www.justiceinitiative.org/uploads/bd50b729-d427-4fbb-8da2-1943ef2a3423/global-principles-national-security-10232013.pdf

Puccinelli, O. (2004). Evolución histórica y análisis de las diversas especies, subespecies, tipos y subtipos de habeas data en América Latina (Un intento clasificador con fines didácticos). *Vniversitas*, *53*(107), 471-501. https://revistas.javeriana.edu.co/index.php/vnijuri/article/view/14792

Rodríguez, R. (2018). El Derecho de Acceso a la información pública como un Derecho Humano Fundamental. *La Revista de Derecho*, *38*, 25–37. https://doi.org/10.5377/lrd.v38i0.5816

Sanz, F. J. (2025). Derecho fundamental a la protección de los datos personales en América Latina: desafíos ante el alcance extraterritorial del Reglamento General de Protección de Datos de la Unión Europea. *Revista derecho del Estado*, (62), 143-169. https://doi.org/10.18601/01229893.n62.06

Sartre, J. P. (1971). *Huis Clos*. Gallimard.

Scheinin, M. (2010). *Recopilación de buenas prácticas relacionadas con los marcos y las medidas de carácter jurídico e institucional que permitan garantizar el respeto de los derechos humanos por los servicios de inteligencia en la lucha contra el terrorismo, particularmente en lo que respecta a su supervisión*. Naciones Unidas. https://docs.un.org/es/a/hrc/14/46

Sentencia C-748 (2011, 6 de octubre). Corte Constitucional de Colombia. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=50042

Upegui, J. C. (2007). Diez ideas para un régimen de datos personales en clave latinoamericana. *Derecho Comparado de la Información*, (10), 133-152. https://revistas-colaboracion.juridicas.unam.mx/index.php/decoin/article/view/33139/30103

Upegui, J. C. (2019). *Transparencia estatal y datos personales: El problema de la publicidad de la información personal en poder del Estado. Estudio comparado México–Colombia* [Tesis de doctorado en Derecho, Universidad Nacional Autónoma de México].

Uprimny, R. (1998). La uni-diversalidad de los derechos humanos: conflictos de derechos, conceptos de democracia e interpretación constitucional. *Pensamiento Jurídico,* (7), 25-39.