

Sentencia C-406/22

Referencia: expediente D-14799

Accionante: Juan Manuel López Molina

Asunto: Acción de inconstitucionalidad contra el artículo 48 (parcial) de la Ley 2197 del 2022, “por medio de la cual se dictan normas tendientes al fortalecimiento de la seguridad ciudadana y se dictan otras disposiciones”.

Magistrada ponente:

CRISTINA PARDO SCHLESINGER

Bogotá D. C., noviembre diecisiete (17) de dos mil veintidós (2022)

La Sala Plena de la Corte Constitucional, en ejercicio de sus atribuciones constitucionales, previo cumplimiento de los requisitos y trámites establecidos en el Decreto 2067 de 1991, profiere la siguiente

SENTENCIA

I. I. ANTECEDENTES

1. 1. En ejercicio de la acción pública consignada en el artículo 241 de la Constitución Política, el ciudadano Juan Manuel López Molina presentó demanda de inconstitucionalidad contra el artículo 48 (parcial) de la Ley 2197 del 2022, “por medio de la cual se dictan normas tendientes al fortalecimiento de la seguridad ciudadana y se dictan otras disposiciones”.

2. La Corte Constitucional resolvió, mediante auto de 6 de junio de 2022, admitir la demanda, en cuanto a la información privada registrada en circuitos cerrados de vigilancia y seguridad privada a la que podrá acceder la Policía Nacional para acciones de prevención, identificación o judicialización y la inadmitió en lo relacionado con la información obtenida en espacio semipúblico o semiprivado.

3. Presentado el escrito de subsanación dentro del término previsto, el despacho sustanciador consideró que el demandante no corrigió el cargo y dictó auto de rechazo que no fue suplicado, con lo que se dio curso a lo previsto en el numeral noveno del auto de inadmisión.

4. Cumplidos los trámites propios de esta clase de procesos, y previo el concepto de la Procuradora General de la Nación, procede la Corte a decidir sobre la demanda de la referencia.

. NORMA DEMANDADA

5. A continuación, se transcribe la norma demandada:

LEY 2197

ENERO 25 DE 2022

Diario Oficial No. 51.928 de enero 25 DE 2022

POR MEDIO DE LA CUAL SE DICTAN NORMAS TENDIENTES AL FORTALECIMIENTO DE LA SEGURIDAD CIUDADANA Y SE DICTAN OTRAS DISPOSICIONES.

EL CONGRESO DE COLOMBIA DECRETA:

(...)

TÍTULO V

NORMAS QUE MODIFICAN Y ADICIONAN LA LEY 1801 DE 2016 - CÓDIGO NACIONAL DE SEGURIDAD Y CONVIVENCIA CIUDADANA

CAPITULO I

(...)

ARTÍCULO 48. Adiciónese el artículo 237B a la Ley 1801 de 2016 Código Nacional de Seguridad y Convivencia Ciudadana, el cual quedara así:

Artículo 237B. Acceso a circuitos de vigilancia y seguridad privada. La Policía Nacional podrá acceder a los circuitos cerrados de vigilancia y seguridad privada, para acciones de prevención, identificación o judicialización.

. DE LA DEMANDA

6. Según el accionante el artículo 48 de la Ley 2197 de 2022 vulnera por omisión legislativa relativa los artículos 15 de la Carta Política, 12 de la Declaración Universal de los Derechos Humanos, 11 de la Convención Americana sobre Derechos Humanos, 17 del Pacto Internacional de Derechos Civiles y Políticos y 4º, 5º y 6º de la Ley Estatutaria 1581 de 2012 “por la cual se dictan disposiciones generales para la protección de datos personales”.

8. A su juicio la norma no incorporó un ingrediente que resultaba imperativo por mandato constitucional expreso y del derecho convencional, a saber: pasó por alto condiciones para evitar intromisiones injustificadas y/o arbitrarias de la Policía Nacional en la información privada captada por circuitos cerrados de vigilancia y seguridad que fue habilitada irrestrictamente para el efecto con fines de prevención, identificación o judicialización, sin que exista razón suficiente que justifique la omisión.

9. Por lo anterior, solicitó que se declare la exequibilidad condicionada de la norma demandada, “en el entendido de que para acceder a dicha información privada la Policía Nacional requerirá de la autorización previa por parte de quien tenga la legitimidad para otorgarla o por autoridad judicial en el cumplimiento de sus funciones”.

10. Con el propósito de profundizar en las razones de su solicitud y luego de analizar la norma acusada precisó que la disposición en ella contemplada habilita a la Policía Nacional para “acceder a circuitos cerrados de vigilancia y seguridad privada, para acciones de prevención, identificación y judicialización”.

11. Advirtió que esto sucede sin tomar nota de que “cierta información privada, que estos sistemas de videovigilancia y seguridad privada registran, como aquella que se encuentra en el ámbito propio del sujeto a quien le incumbe, solo puede ser obtenida con la autorización previa por parte de quien tenga la legitimidad para otorgarla”. Reiteró que, al no prever requisito, autorización previa del titular o permiso de autoridad judicial en el cumplimiento de sus funciones, la norma desconoce el derecho fundamental a la intimidad de los titulares de la información privada.

12. El demandante insistió en que la ausencia de este elemento en la norma acusada permite entender que, con el fin de acceder a la información privada, captada por circuitos cerrados de vigilancia y seguridad privada, la Policía Nacional no precisa autorización alguna y que, si en gracia de discusión la necesitara, la norma podría interpretarse en el sentido de que no la requiere.

13. Observó, asimismo, que el precepto en cuestión tampoco remite a otras disposiciones del Código Penal o de Procedimiento Penal con el propósito de garantizar el derecho fundamental a la intimidad de los titulares de la información y “mucho menos a la Ley Estatutaria 1581 de 2012 o alguna otra esfera del ordenamiento jurídico”.

14. Después de aludir a los alcances del derecho fundamental a la intimidad expresamente reconocido en el artículo 15 superior y de referirse al acceso a la información privada y al manejo de datos sensibles, mostrando los avances incorporados en la Ley Estatutaria 1581 de 2012, el actor resaltó varios de los principales pronunciamientos de la Corte Constitucional en la materia.

15. Acto seguido, se dio a la tarea de justificar los motivos por los cuales presentó como cargo único una omisión legislativa relativa. Se refirió inicialmente a los requisitos que la Corte Constitucional ha fijado para la admisión de este tipo de cargo y solicitó a la Corte que declare la exequibilidad condicionada de la norma acusada, en el sentido de que se exija autorización previa por parte de quien esté legitimado para ello. El desarrollo de la argumentación dirigida a mostrar el cumplimiento de las aludidas exigencias se abordará y analizará con detalle, más adelante, en las consideraciones de la presente sentencia.

. INTERVENCIONES

a. a) Fundación Karisma

16. Para la fundación, el cargo de inconstitucionalidad debe prosperar, pues la norma acusada desconoce el derecho a la privacidad que “otorga los medios para que cada ciudadano ejerza otros derechos como el libre desarrollo de la personalidad y su intimidad, en condiciones de autonomía y dignidad”. Esta idea la sustentó apelando a lo dicho por las Naciones Unidas en su Relatoría sobre el derecho a la privacidad, donde se destaca, además, que éste posibilita gozar de otros derechos.

17. Luego de citar los artículos 28 superior, 13 de la Convención Americana sobre Derechos Humanos y 17 del Pacto Internacional de Derechos Civiles y Políticos, concluyó que facultar a la Policía Nacional con el objeto de facilitarle el acceso “a información contenida en circuitos cerrados de vigilancia y seguridad privada para acciones de prevención, identificación o judicialización sin ningún requisito, autorización previa del titular o permiso de autoridad judicial en el cumplimiento de sus funciones, que garantice el derecho fundamental a la intimidad de los titulares de la información privada, vulnera principios y derechos consagrados en el ordenamiento constitucional e internacional.

18. Por lo anterior, solicitó declarar la exequibilidad condicionada de la norma “en el entendido de que el manejo y tratamiento de información, datos e imágenes a los cuales accede y usa la Policía Nacional a través de los sistemas de vigilancia y seguridad privada, deben observar los principios de legalidad, finalidad, libertad, transparencia, acceso y circulación restringida, seguridad, confidencialidad y caducidad. Estos principios se materializan a través del otorgamiento de la autorización por parte del titular para el tratamiento de datos personales o la existencia de una orden judicial o administrativa”.

19. Puso de presente que en los pronunciamientos de la Corte Constitucional acerca de las cámaras de vigilancia y las restricciones a la intimidad se ha aplicado el juicio de proporcionalidad. Igualmente, señaló que el artículo 48 de la Ley 2197 de 2022 no se ajusta a la Constitución, pues si bien la intervención en el derecho a la intimidad es razonable, no es proporcionada. Esto debido a que no diferencia el tipo de información tratada, desconoce la relación con el derecho al hábeas data y pasa por alto “que el derecho a la intimidad, en todos los espacios, mantiene una esfera de protección”. En fin, la fundación insistió en que, al facultar a la Policía Nacional de manera indistinta, el artículo 48 desconoció el impacto que tiene el acceso a la información de cámaras de vigilancia.

b) Intervención del Ministerio de Justicia y del Derecho

20. La autoridad interviniente también solicitó declarar la exequibilidad condicionada de la norma acusada. En primer lugar, recordó que la Corte Constitucional se pronunció sobre el artículo 237 de la Ley 1801 de 2016 en la sentencia C-094 de 2020. Citó algunos de los apartes de la sentencia, tanto como su parte resolutive y concluyó que tanto las imágenes como los sonidos y las conversaciones de las personas que quedan registrados en las cámaras de vigilancia u otros sistemas pueden calificarse, sin lugar a duda, de datos personales cuyo contenido debe sujetarse a los contenidos del derecho al hábeas data.

21. Con fundamento en lo expuesto, y tras nombrar los artículos 15 y 250 superiores y la Ley Estatutaria de protección de datos personales, concluyó que para que la Policía Nacional acceda a información personal captada por medio de sistemas de seguridad y vigilancia –al margen del lugar en el que estas se encuentren localizadas–, resulta indispensable contar con autorización judicial previa cuando puedan verse afectados derechos fundamentales como el derecho a la intimidad. Con el fin de acceder a esta información deben cumplirse los principios relativos a la protección de datos previstos en el artículo 4º de la Ley Estatutaria 1581 de 2012.

22. En conclusión, solicitó a la Corte proferir una sentencia de exequibilidad condicionada “en relación con la norma acusada y respecto de los cargos señalados en la demanda”.

c) Intervención de la Universidad Externado de Colombia

24. La universidad interviniente afirmó que los derechos afectados, en un primer plano, son el de la intimidad y hábeas data, por lo que el régimen aplicable tendría que ser el del

derecho a la intimidad “en concordancia con el régimen constitucional del derecho a la propiedad privada”. En el segundo plano, los derechos afectados serían el de hábeas data y el de la intimidad. Por ello, advirtió que era necesario tener en cuenta algunas particularidades en el momento de analizar la constitucionalidad del artículo 237B para evitar “que una aplicación mecánica o irreflexiva de los principios constitucionales del hábeas data termine siendo disfuncional”.

25. Con relación al asunto en cuestión señaló que, en el marco constitucional, cualquier intervención en la esfera privada debe estar sujeta a la ley y contar con una justificación amplia que prevenga la posibilidad de actuaciones o espacios caracterizados por la arbitrariedad. Según la universidad interviniente la disposición acusada no cumple esas exigencias, pues habilitó “a la Policía Nacional para realizar una especie de búsqueda selectiva en bases de datos (¿qué otra función se persigue con el “acceso” a estos sistemas sino es, como lo dice la propia disposición, “identificar y judicializar”?). Todo ello sin que se prevean las garantías que la legislación penal y la Jurisprudencia constitucional han establecido para esto, en especial, en la Sentencia C-336 de 2007, MP Jaime Córdoba Triviño”.

26. A propósito de los requerimientos señalados, subrayó, en primer lugar, que no se contaba con un “control jurisdiccional a la actividad de policía con fines de “identificación y judicialización” y destacó su importancia, dado que “esta actividad de policía se concreta en el acceso a información contenida en sistemas de información de carácter privado (primera injerencia en la esfera privada), que pueden tener la característica de información privada o semiprivada de terceros indeterminados (segunda injerencia en la esfera privada), y que por tanto, debería estar sometida a un control judicial, por lo menos, de carácter posterior”.

27. En segundo lugar, que el artículo 237B no previó limitación alguna a la facultad otorgada a la Policía Nacional. En esa línea, no cualificó “el titular de la tecnología”, puesto que autoriza el acceso tanto “a circuitos cerrados de seguridad públicos, como privados” y

tampoco cualificó “el lugar desde el que se recoge la información (espacios públicos, semiprivados, privados, abiertos al público, etc.). Menos aún, “el tipo de información que puede ser accedida (pública, semiprivada, privada)”.

28. Además, frente a la hipótesis de la información privada, agregó que la norma no especificó como límite “la autorización, el ejercicio de la libertad, de quien tenga la ‘legitimidad para otorgar’ el acceso”. Finalmente, concluyó que “si la Corte Constitucional no encontraba mérito para declarar la exequibilidad total del artículo 237B, la decisión se circunscriba de forma clara, precisa y sobre todo explícita, al cargo único de esta demanda”.

d) Intervención de la Universidad Libre

29. La Universidad Libre sostuvo que la norma acusada pasó por alto que el acceso de la Policía Nacional a la información que captan los circuitos cerrados de vigilancia y seguridad privada “debe sujetarse a la autorización previa por parte de quien tenga la legitimidad para otorgarla”. También puso de presente la necesidad de distinguir entre diversas clases de información.

30. La universidad interviniente solicitó a la Corte Constitucional que declare la exequibilidad condicionada del artículo 48 de la Ley 2197 de 2022. Añadió que, en línea con la prohibición prevista en el artículo 7º de la Ley 1581 de 2012, relativa al tratamiento de datos personales de los niños, niñas y adolescentes, -norma que también proscribió el tratamiento de información privada, semiprivada y semipública-, debía establecerse que solo se podría autorizar “el acceso a los circuitos cerrados de vigilancia y seguridad privada para acciones de prevención, identificación y judicialización, siempre y cuando éstos sean de naturaleza pública, y sean autorizados mediante una orden emitida por una autoridad judicial, prohibiendo que una autoridad administrativa pueda otorgar la autorización para acceder a la información privada, semiprivada, o semipública sin el consentimiento del titular de la

misma”.

31. Para establecer qué naturaleza tiene la información captada por circuitos cerrados de televisión, la universidad consideró indispensable tomar nota del lugar en el que se ubican las cámaras de vigilancia. Advirtió que es necesario estudiar cada caso, pues si cámaras de seguridad se instalan por orden legal y/o judicial dentro de una residencia, entonces, afirmó, “no se puede considerar que las imágenes que capten dichos equipos sean de carácter privado, toda vez que, la utilización de dicho material estaría destinada a fines completamente diferentes a los personales”.

32. La universidad interviniente resaltó la importancia de limitar el acceso a las videograbaciones si esta se clasifica en privada, semiprivada y semipública y supeditar su acceso a previa autorización de autoridad judicial, ello con el propósito de “evitar el control social y el riesgo de quebrantar los pilares fundamentales del Estado social de derecho”. En su criterio, posibilitar que las autoridades administrativas autoricen el “acceso a la información semiprivada y semipública sin el consentimiento del titular, configura una sociedad del riesgo y del miedo y es sumamente contraproducente por su carácter nugatorio del derecho a la intimidad” .

33. Con el fin de ilustrar estos peligros trajo a colación que este tipo de autorizaciones normativas abría la puerta para que una sociedad en la que, “por ejemplo, quienes pretenden defender un derecho como la protesta, pued[a]n ser identificados, reseñados y rastreados por las cámaras, para luego ser perseguidos por gobernantes sin escrúpulos, que anteponen las razones de seguridad, por encima de las razones de Estado”.

34. Sobre este extremo, formuló una alerta en relación con lo que la doctrina ha denominado “sociedad panóptica” y solicitó tomar en cuenta el riesgo que se corre cuando se permite a las autoridades administrativas “autorizar el acceso a los datos sensibles de las personas que

se encuentran en los circuitos cerrados de seguridad y vigilancia en espacios privados, semiprivados, y semipúblicos”. Subrayó que esto se traducía en “un as bajo la manga para ejercer la persecución política, moral, social de todos aquellos que piensan u opinan en contra del sistema, al mejor estilo del gran hermano de George Orwell en 1984”. Finalmente, la universidad interviniente solicitó a la Corte declarar la exequibilidad condicionada de la disposición demandada.

. CONCEPTO DE LA PROCURADORA GENERAL DE LA NACIÓN

35. La señora Procuradora se refirió, en primer lugar, a que el acceso a videos que queden registrados en los circuitos cerrados de seguridad y vigilancia se encuentra supeditada a una orden proferida por la autoridad competente o a que el administrador autorice su consulta, según lo dispuso la ley de protección de datos. Sobre este extremo sostuvo que, acorde con pronunciamientos jurisprudenciales, debía “valorarse el lugar de instalación de los equipos de filmación”. En relación con este aspecto, recordó que en la sentencia C-602 de 2016, la Corte reconoció distintos tipos de autorización, dependiendo de la naturaleza de la información. Resaltó que, en atención a la necesidad de proteger el derecho fundamental a la intimidad, podía restringirse el acceso a los videos de los sistemas cerrados de vigilancia y seguridad privada supeditándolo, “en algunos casos, a autorización administrativa o judicial previa”.

36. Para la señora Procuradora esto depende tanto de la ubicación de las cámaras, como de la información que estas estén en capacidad de captar. Señaló, sin embargo, que podía prescindirse de esta autorización, “en casos de flagrancia o imperiosa necesidad, sin perjuicio del control jurisdiccional posterior correspondiente”. Con fundamento en lo señalado, encontró que la demanda de la referencia se encontraba llamada a prosperar, toda vez que concurrían “los presupuestos necesarios para sostener que al expedir el artículo 48 de la Ley 2197 de 2022, el Congreso de la República incurrió en la omisión legislativa alegada por el demandante”.

37. En criterio del Ministerio Público no resulta claro que, so pretexto de “velar por la seguridad ciudadana”, la Policía Nacional pueda acceder a circuitos cerrados de seguridad y vigilancia privada, sin que, previamente, solicite la autorización respectiva, toda vez que, dada su ubicación, estos circuitos están en condición de “captar imágenes relacionadas con información semiprivada, privada o reservada, debido a la posibilidad de afectar gravemente la intimidad de las personas”.

38. Por los motivos expuestos y resaltando el alcance jurisprudencial dado al derecho a la intimidad, la Vista Fiscal solicitó a la Corte Constitucional declarar exequible la disposición acusada “bajo el entendido de que el acceso de la Policía Nacional a los circuitos de vigilancia y seguridad privada ubicados en lugares en los que se puedan captar imágenes o videos relacionados con información semiprivada, privada o reservada de las personas, requerirá de la autorización previa que corresponda en virtud de la naturaleza de los datos, salvo casos excepcionales de flagrancia o imperiosa necesidad en los que se deberá acudir al control jurisdiccional posterior correspondiente”.

. CONSIDERACIONES DE LA CORTE CONSTITUCIONAL

1. 1. Competencia

39. En virtud de lo dispuesto en el artículo 241, numeral 5° de la Carta Política, la Corte Constitucional es competente para conocer de la demanda formulada en contra del artículo 48 (parcial) de la Ley 2197 del 2022, “por medio de la cual se dictan normas tendientes al fortalecimiento de la seguridad ciudadana y se dictan otras disposiciones”.

2. Presentación del caso

40. Según el accionante, el Legislador al expedir la norma acusada –que regula el acceso a circuitos cerrados de vigilancia y seguridad privada por parte de la Policía Nacional para acciones de prevención, identificación o judicialización–, pasó por alto que, tratándose de información privada que, como tal, recae en el ámbito de la intimidad de las personas, la puesta a disposición de esta información debe estar precedida necesariamente de la autorización previa por parte de quien tenga la legitimidad para otorgarla. En ese sentido, consideró que el Legislador incurrió en una omisión legislativa relativa contraria al derecho a la intimidad consignado en la Constitución y que también desconoció los pactos internacionales sobre derechos humanos que garantizan este derecho.

41. La mayoría de las intervenciones y la Vista Fiscal estuvieron de acuerdo en que en el asunto de la referencia se presentaba una omisión legislativa relativa y sugirieron a la Corte declarar la exequibilidad condicionada de la norma acusada, si bien no coincidieron en el sentido de si la autorización para acceder a los circuitos cerrados de vigilancia y seguridad privada la debía dar únicamente el titular de la información previa autorización judicial o también la autoridad administrativa. La Universidad Externado de Colombia propuso declarar inexecutable la norma o, en su defecto, su exequibilidad condicionada ateniéndose estrictamente al cargo analizado.

42. Antes de plantear el problema jurídico y la metodología para resolverlo, procederá la Sala a pronunciarse sobre el contexto normativo en el que se inserta la norma acusada y se referirá, igualmente, a su sentido y alcance.

3. Contexto normativo en el que se inserta el artículo 48 de la Ley 2197 de 2022. Sentido y alcance de la disposición.

43. La Ley 2197 de 2022 forma parte del conjunto normativo que integra la Ley 1801 de 2016 o Código Nacional de Seguridad y Convivencia Ciudadana. Su artículo 48 –demandado en el expediente de la referencia–, tuvo por objeto añadir el artículo 237B a ese sistema y se encuentra precedido del artículo 237 que regula, a su turno, lo concerniente a la integración de circuitos de vigilancia. En alguna de las intervenciones se advirtió la necesidad de tomar en cuenta la diferencia entre el artículo 237 y el artículo 237B, con el propósito de fijar los alcances de la norma acusada y formular el problema jurídico a resolver.

44. Una lectura atenta del artículo 237 permite establecer que las dos normas regulan aspectos diferentes. Mientras el artículo 237 se refirió a la integración de sistemas de vigilancia –se destaca– y puso un acento especial en la ubicación de los sistemas de video y medios tecnológicos o similares, esto es, aludió, específicamente, a aquellos localizados en áreas comunes, lugares abiertos al público o que siendo privados trasciendan al público –con independencia de si son de propiedad privada o pública–, el artículo 237B se pronunció sobre los circuitos cerrados de vigilancia y seguridad privada. –se destaca–.

45. Así, el artículo 237 dejó claro que tratándose de información, imágenes y datos de cualquier índole captados y/o almacenados en los sistemas de video o medios tecnológicos situados como se describió en el numeral (55), serían catalogados como públicos y de libre acceso, salvo que se trate de información amparada por la reserva legal –se destaca–.

46. El inciso segundo del artículo 237 dispuso, asimismo, que los sistemas referidos se enlazarán de manera temporal a la red que, para ese fin, disponga la Policía Nacional, de acuerdo con la reglamentación expedida por el Gobierno Nacional. Lo anterior, exceptuando los sistemas destinados a la Defensa y Seguridad Nacional. También dispuso que, tratándose de sistemas de video y medios tecnológicos o similares instalados en áreas comunes, lugares abiertos al público o que siendo privados trasciendan a lo público, requerirán autorización previa por parte de quien tenga la legitimidad para otorgarla –se destaca–.

47. Pese a los aspectos en común que presentan los artículos 237 y 237B, también es factible constatar elementos que denotan sus diferencias, como se verá a continuación.

48. En el supuesto previsto por el artículo 237B se faculta a la Policía Nacional para acceder a la información registrada o almacenada en circuitos cerrados de seguridad y vigilancia privada con unos propósitos, a saber, para acciones de prevención, identificación o judicialización. En ese sentido, la atribución concedida a la Policía Nacional en relación con información captada por tales circuitos tiene mayores alcances, pues la posibilidad de acceder a ella por parte de la Policía Nacional no se sujeta a ningún condicionamiento o restricción.

49. A lo anterior se suma que se trata de tipos de tecnología diferentes. En el artículo 237 se hace referencia a “sistemas de video y medios tecnológicos, o los que hagan sus veces”, mientras que en el artículo 237B se alude a “circuitos cerrados de vigilancia y seguridad privada”. En el caso del artículo 237 la titularidad de los equipos puede ser pública o privada, pero su ubicación debe ser pública –y de ser privada– debe trascender a lo público. En el 237B se trata de circuitos de vigilancia y seguridad privada, esto es, cuyas propietarias son personas naturales o jurídicas y no el Estado.

50. Además, si bien las dos normas le atribuyen facultades a la Policía Nacional, –en el artículo 237 “enlazar” los sistemas de video y medios tecnológicos, o los que hagan sus veces, de propiedad privada o pública de manera permanente o temporal a la red que para tal efecto esa autoridad disponga– y en el artículo 237B –“acceder” a circuitos cerrados de seguridad y vigilancia privada para acciones de prevención, identificación o judicialización–, es claro que en el primer caso se enfatizó el carácter público de la ubicación del sistema o la trascendencia pública de la ubicación privada, mientras que, en el segundo, se trata exclusivamente de circuitos cerrados de vigilancia y seguridad privada sin mayor

determinación o precisión.

51. El artículo 237 establece ciertas restricciones que no se encuentran de ninguna manera previstas en el artículo 237B. Así, en su inciso primero el artículo 237 se abstuvo de calificar como pública y de libre acceso, “la información amparada por reserva legal”. En el inciso segundo también hizo una salvedad, esta vez, referente a los sistemas de video y medios tecnológicos –o los que hagan sus veces– que estén “destinados para la Defensa y Seguridad Nacional”. Estos últimos, así se encuentren instalados “en espacio público, áreas comunes, lugares abiertos al público o que siendo privados trasciendan a lo público”, no se enlazarán “de manera permanente o, temporal, a la red que para tal efecto disponga la Policía Nacional”. Adicionalmente, el referido enlace se sujetó a la “reglamentación que para tal efecto disponga el Gobierno Nacional”.

52. Finalmente, el párrafo del artículo 237 también incluyó un condicionamiento, a saber, que para el enlace aludido se requiere autorización previa por parte de quien tiene legitimidad para otorgarla cuando se trate “de sistemas instalados en áreas comunes, lugares abiertos al público o que siendo privados trasciendan a lo público” –se destaca-. Mientras tanto, el artículo 237B se redujo a afirmar que “[l]a Policía Nacional podrá acceder a los circuitos cerrados de vigilancia y seguridad privada, para acciones de prevención, identificación o judicialización”, sin imponer una condición o exigencia adicional.

53. Por otro lado, es importante advertir que la disposición contemplada en el artículo 237 fue objeto de demanda de inconstitucionalidad y la Corte resolvió declarar la exequibilidad condicionada de la norma, mediante la sentencia C-094 de 2020. En aquella ocasión la Sala hizo un conjunto de precisiones.

54. En primer lugar, destacó que “la naturaleza de la información captada por las cámaras no depende del lugar en el que estas son instaladas” –se destaca-. Por eso, consideró

problemática la redacción de la disposición contemplada en el artículo 237, pues recordó que, al margen de su ubicación, la Constitución prohibía, en general, la existencia de sistemas de vigilancia cuyo propósito o consecuencia fuera la de quebrantar el derecho a la intimidad, desconocer el derecho al hábeas data o impedir el ejercicio de las libertades constitucionalmente protegidas –se destaca–.

55. La sentencia aplicó la metodología de la armonización concreta y, en ese sentido, fijó el alcance del artículo 237 a la luz del régimen constitucional y legal de protección de datos personales, por una parte, y de las reglas fijadas por la jurisprudencia en relación con distintos tipos de información, por la otra. Encontró que la medida analizada buscaba cumplir una finalidad legítima, esto es, hacer prevalecer el interés general y garantizar el orden público. Sin embargo, reconoció que materializar ese objetivo generaba tensiones.

56. Por eso, en la parte resolutive de la sentencia decidió declarar la exequibilidad condicionada del artículo 237 de la Ley 1801 de 2016 por el cargo analizado, “en el entendido de que el manejo y tratamiento de información, datos e imágenes captados y/o almacenados a través de sistemas de video o medios tecnológicos que estén ubicados o instalados en el espacio público, en lugares abiertos al público, en zonas comunes o en lugares privados abiertos al público o que siendo privados trasciendan al público, deberán observar los principios de legalidad, finalidad, libertad, transparencia, acceso y circulación restringida, seguridad y confidencialidad y caducidad, en los términos del numeral 157 de esta providencia”.

57. A propósito de esa decisión, la Corte aclaró que la tarea de captar o almacenar información, datos o imágenes de que trata el artículo 237 debía ceñirse íntegramente a los principios previstos en la Ley 1581 de 2012. En particular, debía establecerse un término para la conservación de la información, fijarse qué obligaciones se derivan en relación con su tratamiento y, al paso, definir entre qué personas puede circular.

58. Adicionalmente, consideró que resultaba preciso especificar los términos en los que tendría lugar el tratamiento de la información, de modo que no vulnere el derecho al hábeas data. En ese sentido, subrayó que el uso de esa información debía cumplir con los principios y garantías adscritos al derecho de hábeas data previsto en el artículo 15 superior y a los principios a los que se refirió la Corporación en la sentencia C-1011 de 2008.

59. Ahora bien, de lo dicho en precedencia resulta claro que los artículos 237 y 237B son normas que regulan supuestos de hecho diferentes, aluden a diversas tecnologías y tienen distintos alcances.

60. Al respecto, es importante insistir en que el artículo 237B se refiere a un tipo de tecnología específico, a saber, los circuitos cerrados de vigilancia y seguridad privada lo que excluye otras tecnologías de vigilancia tales como las cámaras corporales, drones o cámaras que no operen en circuito cerrado –se destaca-. Cabe anotar, asimismo, que el artículo 237B no distingue varios aspectos, como sí lo hace el artículo 237. Primero, los espacios para la ubicación de las cámaras. Segundo, la clase de información a la que se puede acceder. Tercero, mientras el artículo 237 prevé un conjunto de restricciones, el artículo 237B faculta a la Policía Nacional de manera incondicionada e irrestricta –se destaca-. Estos aspectos ponen de presente que la habilitación contemplada en el artículo 237B es diferente y, sin duda, más amplia que la prevista en el artículo 237.

61. En fin, el artículo 48 de la Ley 2197 de 2022 –que adicionó el artículo 237B a la Ley 1801 de 2016 (Código Nacional de Seguridad y Convivencia Ciudadana)– otorgó a la Policía Nacional la facultad de realizar el tratamiento de datos personales en dos modalidades. Primero, en el “acceso” a los datos registrados en circuitos cerrados de vigilancia y seguridad privada. Segundo, en el “uso” de estos datos para unos determinados objetivos, a saber, de prevención, identificación o judicialización.

62. El accionante consideró en su escrito de demanda que como la facultad atribuida por la norma acusada a la Policía Nacional no se condicionó ni se sujetó a restricción alguna, el Legislador habría incurrido en una omisión legislativa relativa que, en su criterio, desconocería el derecho fundamental a la intimidad, especialmente protegido en el plano interno e internacional, así como la Ley Estatutaria 1581 de 2012 “por la cual se dictan disposiciones generales para la protección de datos personales”. El actor se refirió concretamente el artículo 4º de la mencionada ley estatutaria y a la sentencia C-602 de 2016 para fundamentar la acción constitucional.

63. Con base en la demanda formulada, a continuación, la Sala indagará si el actor cumplió con la carga argumentativa exigida cuando se formula una omisión legislativa relativa. Previo a responder este interrogante, la Corte reiterará su jurisprudencia sobre este tema.

4. Cuestión previa: del cargo por omisión legislativa relativa: ¿cumplió el accionante con las exigencias previstas por la jurisprudencia constitucional para alegarlo?

a. a) Reiteración de jurisprudencia

64. Esta Corporación ha insistido en que el legislador desconoce la Constitución por omisión cuando se echa de menos “una regulación normativa de materias sobre las cuales tiene una específica y concreta obligación de hacer, determinada por el constituyente. De este modo y, de manera excepcional, el silencio del legislador puede ser objeto de control jurisdiccional por medio de la acción pública de inconstitucionalidad en la que se alegue una omisión legislativa de carácter relativo. Con todo, debe anotarse que, invariablemente, la Corte ha reiterado su incompetencia para pronunciarse sobre omisiones legislativas absolutas.

65. La jurisprudencia constitucional ha sostenido de manera constante que se está ante una omisión legislativa relativa cuando el legislador regula o construye una institución, pero omite una “condición o un ingrediente que, de acuerdo con la Constitución, sería exigencia esencial para armonizar con ella”.

66. Teniendo en cuenta que las omisiones pueden ocurrir de diferentes maneras, la jurisprudencia las ha descrito así: a) “cuando expide una ley que, si bien desarrolla un deber impuesto por la Constitución, favorece a ciertos sectores y perjudica a otros”; b) “cuando adopta un precepto que corresponde a una obligación constitucional, pero excluye expresa o tácitamente a un grupo de ciudadanos de los beneficios que otorga a los demás”; y c) “cuando al regular una institución omite una condición o un elemento esencial exigido por la Constitución” –se destaca–.

67. En todo caso, tras admitir la posibilidad excepcional del desconocimiento de la Carta Política por omisiones legislativas relativas, la jurisprudencia constitucional ha puesto énfasis en que el cargo por este concepto debe cumplir con exigencias que se han ido decantando con el paso del tiempo y que se circunscriben, entre otras, a las siguientes:

(i) Que exista una norma sobre la cual se predique necesariamente el cargo, y que ‘(a) excluya de sus consecuencias jurídicas aquellos casos equivalentes o asimilables o, en su defecto, (b) que no incluya determinado elemento o ingrediente normativo’.

(ii) Que exista un deber específico impuesto directamente por el Constituyente al Congreso de la República que resulta omitido, ‘por (a) los casos excluidos o (b) por la no inclusión del elemento o ingrediente normativo del que carece la norma’. Esto, por cuanto sólo se configura una omisión legislativa relativa cuando el legislador incumple una concreta ‘obligación de hacer’ prevista en la Constitución;

(iii) Que la exclusión tácita o expresa de los casos o ingredientes carezca de una razón suficiente, lo cual implica verificar si ‘el hecho de omitir algún elemento al momento de proferir la norma no hizo parte de un ejercicio caprichoso del legislador, sino, por el contrario, estuvo fundado en causas claras y precisas que lo llevaron a considerar la necesidad de obviar el aspecto que se echa de menos por los demandantes’; y,

(iv) Que la falta de justificación y objetividad de la exclusión genere una desigualdad negativa frente a los que se encuentran amparados por las consecuencias de la norma.

Esta última exigencia es aplicable sólo en aquellos casos en los que se afecte el principio de igualdad, es decir, “cuando la norma incompleta se evidencia discriminatoria al no contemplar todas las situaciones idénticas a la regulada, o, dicho en otras palabras, cuando no se extiende un determinado régimen legal a una hipótesis material semejante a la que termina por ser única beneficiaria de este”.

En este sentido, la Sala ha advertido que, con el propósito de constatar la concurrencia de la última exigencia, es necesario verificar la razonabilidad de la diferencia de trato, esto es, valorar ‘(a) si los supuestos de hecho en que se encuentran los sujetos excluidos del contenido normativo son asimilables a aquellos en que se hallan quienes sí fueron incluidos, y (b) si adoptar ese tratamiento distinto deviene necesario y proporcionado con miras a obtener un fin legítimo’.

68. Como se desprende de lo expuesto, la Corte ha insistido en que si se presenta un cargo por omisión legislativa relativa se exige a quien demanda una mayor carga argumentativa, “en aras de mantener la separación de poderes. Adicionalmente, ha admitido que el remedio en un caso de estos se obtiene por medio de dictar “una sentencia integradora en la que se declara la exequibilidad condicionada del precepto acusado, en el entendido de que éste debe además comprender aquellos supuestos que fueron indebidamente excluidos por el

legislador". Específicamente, la Sentencia C-043 de 2003, explicó que las omisiones legislativas relativas que resulten inconstitucionales pueden ser subsanadas mediante una sentencia integradora. Esta medida le permite al Tribunal Constitucional llenar los vacíos dejados por el legislador, con el fin de armonizar la disposición con el ordenamiento superior.

69. Expuestos los requisitos previstos por la jurisprudencia constitucional para admitir cargos por omisión legislativa relativa, procede la Sala a examinar si en el expediente de la referencia el demandante cumplió con la carga argumentativa exigida.

b) En el asunto que se examina el accionante cumplió con la carga argumentativa exigida para formular una demanda de inconstitucionalidad por omisión legislativa relativa

70. Considera la Sala que la demanda exhibió un desarrollo argumentativo completo, claro y coherente dirigido a mostrar, de manera comprensible y jurídicamente fundada, por qué en este caso se presenta, en su criterio, una omisión legislativa relativa que desconocería el derecho fundamental a la intimidad, especialmente protegido en el plano interno e internacional, así como la Ley Estatutaria 1581 de 2012 "por la cual se dictan disposiciones generales para la protección de datos personales".

71. Primeramente, el accionante advirtió que se cumplía el requisito según el cual debe existir una norma en relación con la que se predica la ausencia o no inclusión de un ingrediente normativo. En su criterio, esta norma es el artículo 48 de la Ley 2197 de 2022, precepto que adicionó un artículo 237B a la Ley 1801 de 2016 o Código Nacional de Seguridad y Convivencia Ciudadana, al tenor de la cual la Policía Nacional "podrá acceder a los circuitos cerrados de vigilancia y seguridad privada, para acciones de prevención, identificación y judicialización".

72. Hizo hincapié en que de la norma mencionada no era factible desprender la necesidad de cumplir con un requisito o autorización previa del titular o de la autoridad judicial en el cumplimiento de sus funciones, dirigido a proteger el derecho fundamental a la intimidad de los titulares de la información privada que se encuentre registrada en circuitos cerrados de vigilancia y seguridad privada.

73. Insistió en que, por el contrario, la norma en cuestión daba “a entender que la Policía Nacional está facultada para acceder a este tipo de información de naturaleza privada sin que se garantice el derecho fundamental a la intimidad de sus titulares y, en ese sentido, que el titular de la información estaría en el deber jurídico de soportar esta restricción a su esfera íntima”, de manera que contradice el ordenamiento jurídico nacional e internacional y es, por consiguiente, arbitraria y desproporcionada, pues, –recalcó–, tampoco suple el vacío de regulación que se presenta con la remisión a otra disposición normativa, bien sea el Código Penal o el Código de Procedimiento Penal y menos la Ley Estatutaria 1581 de 2012.

74. En segundo término, puntualizó sobre la existencia de un deber específico impuesto directamente por el legislador y, para tal efecto, aludió no solo a las normas que integran el bloque de constitucionalidad, sino también a la jurisprudencia constitucional que se pronuncia sobre la obligación de que, tratándose de información privada –se destaca–, se proteja debidamente el derecho fundamental a la intimidad de quienes son titulares de esta clase de información que se halla “en el ámbito propio del sujeto a quien le incumbe y, por ende, sólo puede accederse a esta con la autorización previa por parte de quien tenga la legitimidad para otorgarla”.

75. El accionante invocó, particularmente, el principio de libertad para el tratamiento de datos personales previsto en el artículo 4º de la Ley Estatutaria 1581 de 2012 que, como se conoce, sirve de referente para el control de constitucionalidad y establece que “los datos personales no podrán ser obtenidos o divulgados sin previa autorización, o en ausencia de mandato legal o judicial que releve el consentimiento”. Además, mencionó la sentencia

C-602 de 2016, en la que la Corte afirmó que el acceso a la información privada “sólo puede ser obtenida y ofrecida por orden de autoridad judicial en el cumplimiento de sus funciones”.

76. En tercer lugar, mostró que el Legislador carecía de un principio de razón suficiente para “desconocer la obligación de establecer algún requisito, autorización previa del titular o permiso de autoridad judicial competente para que la Policía Nacional pueda acceder a la información captada (i) por las cámaras de seguridad instaladas en el domicilio de una persona, la cual, en su criterio, es indiscutiblemente privada; (ii) por los equipos de vigilancia instalados en establecimientos privados abiertos al público, en la medida en que, a su juicio, estos tienen también naturaleza privada, debido a que continuamente se encuentran registrando información de las personas que frecuentan ese tipo de lugares”.

77. Para el actor resulta irrazonable y carece de justificación en el ordenamiento constitucional y convencional, que no exista en la norma acusada una previsión dirigida a garantizar la protección del derecho fundamental a la intimidad de que son titulares las personas. Esta ausencia de garantías contraría también el bloque de constitucionalidad en el que se incorporan normas según las cuales “nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada, en la de su familia, en su domicilio o en su correspondencia, ni de ataques ilegales a su honra o reputación y que toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques”.

78. De otra parte, puso de presente que la omisión legislativa relativa en el asunto que se examina es el resultado de la inobservancia del deber específico impuesto por el constituyente al legislador de garantizar la vigencia de los derechos fundamentales, en este caso, el derecho fundamental a la intimidad de aquellas personas que son titulares de la información y quienes no se encuentran “en el deber jurídico de soportar esa restricción en su esfera íntima”.

79. Adicionalmente, recordó que, según la jurisprudencia constitucional, cuando se constata la existencia de una omisión legislativa relativa, es factible “modular el contenido de la sentencia, al extender las consecuencias normativas que el legislador no incluyó injustificadamente”, para que se “mantenga en el ordenamiento el contenido que, en sí mismo, no resulta contrario a la Carta, pero incorporando a este aquel aspecto omitido, sin el cual la disposición es incompatible con la Constitución”.

80. Con fundamento en lo expuesto, considera la Sala que, en el presente asunto, el accionante cumplió con la carga exigida por la jurisprudencia constitucional cuando se formula un cargo por omisión legislativa relativa.

5. Problema jurídico y metodología para resolverlo

81. Teniendo en cuenta el alcance del artículo 48 de la Ley 2197 de 2022 y considerando que el accionante cumplió con la carga exigida por la jurisprudencia constitucional cuando la demanda versa sobre la presencia de una omisión legislativa relativa, le corresponde a la Sala establecer si el Legislador al expedir la norma acusada que i) permitió el acceso irrestricto de la Policía Nacional a circuitos cerrados de vigilancia y seguridad privada en la que datos de personas determinadas o indeterminadas quedan almacenados o registrados y, además, ii) atribuyó a esta autoridad la potestad ilimitada e irrestricta de usar esos datos para acciones de prevención, identificación o judicialización, incurrió, presuntamente, en una omisión legislativa relativa que habría vulnerado los derechos fundamentales a la intimidad y al hábeas data (protección de datos personales) y, en ese sentido, estaría desconociendo los artículos 15 de la Carta Política, 12 de la Declaración Universal de los Derechos Humanos, 17 del Pacto Internacional de Derechos Civiles y Políticos, así como 4º, 5º, y 6º de la Ley Estatutaria 1581 de 2012?

82. Con el objetivo de resolver el problema jurídico, la Sala recordará el alcance de los

derechos fundamentales a la intimidad y al hábeas data en la jurisprudencia constitucional. Además, reiterará sus pronunciamientos en torno a las fronteras constitucionales y legales a las que se sujeta la Policía Nacional en su rol de Policía Judicial y las limitaciones que ha trazado en relación con las empresas privadas que prestan el servicio de vigilancia y seguridad. De otra parte, se pronunciará respecto de la tecnología vinculada con circuitos cerrados de vigilancia y seguridad privada, su regulación jurídica, los riesgos que se enfrentan con su uso y la importancia de acotar los objetivos o fines que justifican el acceso a esta tecnología para que pueda considerarse una acción legítima en un Estado que se rige por las libertades y derechos de la ciudadanía y que evita instrumentalizar a las personas. Igualmente, se referirá a los criterios fijados por la jurisprudencia constitucional para ponderar el conflicto entre, de un lado, la seguridad y la vigilancia y, del otro, los derechos fundamentales a la intimidad y al hábeas data, cuya vigencia se relaciona, estrechamente, con la necesidad de respetar la dignidad humana, la libertad y la autonomía de las personas. Por último, se realizará el examen de constitucionalidad de la norma acusada.

6. Derechos fundamentales que se desprenden del artículo 15 constitucional

83. De la lectura del artículo 15 superior, la jurisprudencia constitucional ha derivado tres derechos fundamentales autónomos: el derecho a la intimidad, el derecho al buen nombre y el derecho al hábeas data. Diferenciar y delimitar estos tres derechos fundamentales ha sido una tarea a la que la Corte le ha conferido la mayor importancia. Lo anterior, por tres motivos. En primer lugar, porque de esta manera se obtiene la protección judicial de estos derechos mediante la acción de tutela. En segundo término, por las diferencias que denotan los ámbitos de protección respectivos y, finalmente, dadas las especificidades del régimen jurídico aplicable y las distintas normas para solucionar un posible conflicto con el derecho a la información u otros bienes jurídicamente protegidos como la seguridad y el orden público. En el presente asunto la Sala reiterará su jurisprudencia en relación con el derecho a la intimidad y el derecho al hábeas data.

a) El derecho a la intimidad en la jurisprudencia constitucional

84. El derecho a la intimidad recibe en nuestro ordenamiento una doble protección nacional e internacional. La Corte ha reiterado en su jurisprudencia que “toda persona tiene derecho a una esfera privada fuera del alcance de las demás personas y del Estado”. Se trata de un “espacio personal ontológico, reservado para cada persona que le permite desarrollarse de forma libre y autónoma”.

85. La Corporación también ha caracterizado el derecho a la intimidad como aquel que preserva una esfera de privacidad en la vida de cada uno/a o de su familia, resguardada de interferencias arbitrarias y/o injustificadas. Desde muy temprano, resaltó que la protección de la intimidad consiste en un modo de garantizar “la paz y la tranquilidad que exige el desarrollo físico, intelectual y moral de las personas, vale decir, como un derecho de la personalidad”, cuya titularidad corresponde a todas y a cada una/uno de quienes gozan a priori de este derecho.

86. En consonancia con lo anterior, la Corte ha sostenido, asimismo, que el derecho fundamental a la intimidad es una esfera que permanece y debe mantenerse refractaria a interferencias externas, con el fin de asegurar que las personas no sean obligadas “a escuchar o a ver lo que no desean escuchar o ver” y tampoco sean compelidas a ser escuchadas o vistas cuando no quieren ser escuchadas o vistas. Es, además, un derecho que se proyecta en distintas facetas de la vida humana y repercute tanto en las “relaciones familiares, las costumbres, la salud, el domicilio, las comunicaciones personales” , como en las creencias religiosas.

87. Por eso la Corte ha destacado que el derecho a la intimidad ofrece condiciones imprescindibles para que una persona participe en la vida social, política, cultural, creando vínculos con su comunidad y, al mismo tiempo, asegurándose así “un reducto o espacio físico

inexpugnable, en el que le es posible encontrar el recogimiento necesario para proyectar libre y autónomamente su personalidad, sin intromisiones no queridas de la vida en sociedad”.

88. En el sentido anotado, la jurisprudencia constitucional ha identificado distintas dimensiones del derecho a la intimidad. Por un lado, la dimensión individual que comprende la privacidad personal y familiar. Este ámbito está protegido “frente a la divulgación no autorizada de los asuntos que conciernen al ámbito de privacidad”. Por otra parte, la dimensión relacional que se conecta con la vida personal, espiritual y cultural. A propósito de este aspecto la jurisprudencia constitucional ha reiterado que el derecho fundamental a la intimidad impone tres tipos de protección, siendo mayor aquella que se da en el terreno personal, media en el ámbito familiar y menor en el campo social.

89. Con todo, la jurisprudencia constitucional ha precisado que la garantía del derecho a la intimidad en ninguna de sus facetas y, menos en la relacionada con la privacidad, puede identificarse ni equipararse a la protección de este derecho en un espacio físico concreto -se destaca-. Como quedó dicho líneas atrás, esta precisión fue reiterada en la sentencia C-094 de 2020, mediante la cual la Corte Constitucional declaró condicionalmente exequible el artículo 237 del Código Nacional de Seguridad y Convivencia Ciudadana.

90. En esta oportunidad, debe insistirse en que la protección de la intimidad es un derecho personalísimo y su protección abarca múltiples dimensiones de la vida, las cuales -dada su importancia-, han de quedar especialmente resguardadas de la publicidad o de intromisiones injustificadas de terceros o del Estado.

91. Ello es así, no solo porque estos bienes le incumben únicamente a cada persona en su singularidad, sino, además, por cuanto significan un “prerrequisito para la construcción de la autonomía individual que a su vez constituye el rasgo esencial del sujeto democráticamente activo”. Por ello esta Corporación ha insistido en que “la clasificación de un espacio como

‘público’ no equivale a una sustracción de este del ámbito de protección del derecho a la intimidad, pues el espacio como tal no determina por sí solo el contenido y alcance de este derecho” –se destaca–.

92. Según la Corte, la extensión con que se protege el derecho fundamental a la intimidad dependerá del grado en que el Estado y todas las personas, sin excepción, observen los límites o exigencias básicas que aseguran respetar y proteger la vida personalísima de cada cual. Honrar estas restricciones evita incurrir en actuaciones dirigidas a interferir arbitraria o injustificadamente en la órbita que cada uno se ha reservado para sí misma/o y previene que se divulguen o se presenten circunstancias personales aptas para desconocer sus derechos fundamentales a la intimidad, a la honra y al buen nombre.

93. Por otra parte, la jurisprudencia ha destacado dos aspectos del derecho fundamental a la intimidad. Uno negativo, esto es, refractario a interferencias arbitrarias y a la divulgación ilegítima de datos que se traduce en la obligación de abstención atribuida a las autoridades y a terceras personas y otro aspecto positivo que se concretiza por medio de acciones y/o medidas normativas, judiciales y administrativas dirigidas a materializar este derecho.

94. La jurisprudencia ha reiterado igualmente que se vulnera el derecho fundamental a la intimidad cuando se presenta una intromisión o injerencia injustificada constitucionalmente en el campo que su titular ha reservado para sí, tanto como cuando –sin existir motivos constitucionalmente legítimos– se divulgan o hacen públicos hechos que son veraces y ciertos, pero no susceptibles de ser compartidos mientras no se cuente con autorización previa de su titular o de autoridad competente.

95. Adicionalmente, resulta importante destacar que el derecho fundamental a la intimidad solo puede ser objeto de limitaciones o restricciones si i) estas se encuentran constitucionalmente justificadas; ii) existe autorización de quien tiene la titularidad del

derecho o iii) se presenta orden proferida por una autoridad competente. Sobre este aspecto se volverá más adelante en esta providencia.

96. Por lo pronto es relevante subrayar que la jurisprudencia también ha destacado la necesidad de proteger el derecho a la expectativa legítima o razonable de intimidad. Este concepto ha sido desarrollado en el derecho comparado, vb.gr., por la Corte Suprema de los Estados Unidos y por el Tribunal Europeo de Derechos Humanos.

97. En el marco de los pronunciamientos realizados por la Corte Suprema de los Estados Unidos ha predominado la tesis según la cual “en el hogar de una persona se espera privacidad”. Por el contrario, no estarían protegidos con esa expectativa “objetos, actividades o declaraciones que [la persona] exponga a plena vista de terceros, porque no ha sido exhibida ninguna intención de dejarlos para sí misma”. Tampoco sería razonable catalogar como expectativa legítima de intimidad conversaciones abiertas. Es de anotar la importancia que adquiere que la persona “exhiba una intención de dejar para sí misma ciertos asuntos”.

98. Especialmente relevante es el pronunciamiento hecho por la Corte Suprema de los Estados Unidos en la sentencia *United States vs. Kyllo* (2001). En aquella ocasión el alto tribunal sostuvo que valerse de imágenes térmicas para irrumpir en el domicilio de una persona no respetaba la expectativa razonable de intimidad y que, para ese fin, resultaba indispensable requerir orden judicial. En esta providencia se puso de manifiesto que el domicilio de las personas “se encuentra plenamente protegido por el derecho a la intimidad y por ello se requiere orden judicial, así no se ingrese en el mismo sino se utilice tecnología para hacer un escaneo termal”.

99. A su turno, el Tribunal Europeo de Derechos Humanos se ha valido de un juicio de expectativa razonable de intimidad, que se realiza de conformidad con las circunstancias del caso concreto y consta de dos etapas. La primera analiza si existe una injerencia en la vida

privada, acorde con la expectativa subjetiva de intimidad. La segunda, indaga sobre la naturaleza de la medida y examina, más concretamente, si la intervención es necesaria en una sociedad democrática para garantizar la seguridad y prevenir el crimen, así como los derechos de otras personas.

100. La Corte Constitucional y la Corte Suprema de Justicia también se han valido de este concepto en su jurisprudencia. Especialmente importante es la sentencia proferida por la Corte Suprema de Justicia el 5 de junio de 2013, mediante la cual se examinó la legalidad de un conjunto de acciones de la Policía Nacional, entre ellas, una requisita preventiva que permitió incautar sustancias, seguido de lo cual esta autoridad ingresó en un predio cercado, pero con el portón principal abierto.

101. En aquella oportunidad la Corte consideró que debía diferenciar dos situaciones. Por un lado, la incautación, respecto de la cual encontró que no vulneró el derecho a la intimidad en tanto se efectuó “en la vía pública como parte de un procedimiento para conjurar una actividad delictiva”. Frente al ingreso al inmueble consideró que no se presentó propiamente en la vivienda, sino en partes del predio donde se tenían cultivos y frente a las cuales no se tenía expectativa de intimidad. En este sentido, la Corte señaló que la inviolabilidad del domicilio comprende en principio la vivienda y la ampliación solo opera cuando exista una expectativa razonable de intimidad.

102. Como se desprende de lo expuesto la protección del derecho fundamental a la intimidad se convierte, en ocasiones, en presupuesto para realizar otros derechos fundamentales cuya importancia resulta crucial. Entre estos se encuentran, por ejemplo, el derecho a que se respete la dignidad humana, el derecho a resguardar la propia imagen, el derecho a la inviolabilidad del domicilio, el derecho al libre desarrollo de la personalidad, para mencionar solo algunos de los más importantes.

b) Derechos estrechamente relacionados con el derecho a la intimidad

i. i) El derecho a la dignidad humana en la jurisprudencia constitucional

103. En desarrollo del artículo 1º superior, esta Corporación ha precisado que la dignidad equivale al merecimiento de un trato especial que tiene toda persona por el hecho de ser tal. “Equivale, sin más, a la facultad que tiene toda persona de exigir de los demás un trato acorde con su condición humana”.

104. Además, la Corte ha precisado que el contenido de la dignidad humana se expresa en dos sentidos. De una parte, desde el objeto concreto de protección y, de otra, a partir de su funcionalidad normativa. En relación con el primero, la jurisprudencia constitucional ha distinguido, entre otros, tres criterios i) “[l]a dignidad humana entendida como autonomía o como posibilidad de diseñar un plan vital y de determinarse según sus características (vivir como quiera)”; ii) “[l]a dignidad humana entendida como ciertas condiciones materiales concretas de existencia (vivir bien)” y iii) “la dignidad humana entendida como intangibilidad de los bienes no patrimoniales, integridad física e integridad moral (vivir sin humillaciones)”.

105. A la luz de la funcionalidad normativa de la expresión, la jurisprudencia constitucional ha identificado asimismo tres criterios: i) “[l]a dignidad humana entendida como principio fundante del ordenamiento jurídico y por tanto del Estado, y en este sentido la dignidad como valor” ; ii) “[l]a dignidad humana entendida como principio constitucional” y iii) “[l]a dignidad humana entendida como derecho fundamental autónomo” .

106. En criterio de esta Corporación la dignidad humana también se erige como un derecho fundamental de eficacia directa, cuyo reconocimiento general compromete el fundamento político del Estado. Por tanto, se traduce en i) “el merecimiento de un trato especial que tiene toda persona por el hecho de ser tal” ; y ii) “la facultad que tiene toda persona de exigir

de los demás un trato acorde con su condición humana” .

107. La jurisprudencia constitucional suele destacar la estrecha relación que existe entre el derecho a la intimidad y la posibilidad de llevar una vida en condiciones de dignidad, esto es, aquella en la cual la persona es un fin en sí misma. Esto ocurre, por lo general, cuando la Corte se pronuncia sobre el núcleo esencial del derecho a la intimidad y sostiene que este “supone la existencia y goce de una órbita reservada a cada persona, exenta del poder de intervención del Estado o de las intromisiones arbitrarias de la sociedad, que le permita a dicho individuo el pleno desarrollo de su vida personal, espiritual y cultural”. La jurisprudencia constitucional ha destacado, incluso, que también en la vida pública hay aspectos íntimos susceptibles de ser protegidos.

108. Así, pese a la existencia de distintas maneras de fijar el sentido y alcance del derecho fundamental a la intimidad, algunos elementos permiten detectar que una parte central de la dignificación de las personas se encuentra relacionada con el derecho a no ser expuestas a observación o escuchas ni objeto de intromisiones indeseadas en el ámbito que pretenden preservar y ocultar para ponerlo fuera del conocimiento ajeno o público, salvo decisión en contrario. En este último caso, esto es, cuando la persona resuelve libremente exhibir los asuntos que forman parte del núcleo de su intimidad al público, entonces ya no sería razonable ni legítimo reclamar discreción frente a la posibilidad del conocimiento ajeno.

) El derecho a resguardar la propia imagen en la jurisprudencia constitucional

109. Para la Corte el derecho a resguardar la propia imagen es un derecho fundamental autónomo “de índole personalísima de raigambre constitucional cuya protección se traduce específicamente en lograr que la imagen continúe siendo la expresión directa de la individualidad e identidad de las personas”. El reconocimiento de este derecho como fundamental se realizó en la sentencia T-405 de 2007. La Corporación ha derivado de esta

aproximación conceptual la necesidad de que “el uso de la imagen propia sea autorizado previamente por su titular, así que las características y manifestaciones externas de la individualidad corporal no puedan ser objeto de libre e injustificada disposición o manipulación por parte de terceros”.

110. Los diversos aspectos desarrollados por la jurisprudencia constitucional permiten concluir que el derecho a resguardar la propia imagen implica que su uso es factible únicamente si media consentimiento previo. Tal exigencia se convierte en una forma de garantizar “la propia imagen como expresión directa de la individualidad e identidad de las personas”. De esta manera, los rasgos que se convierten en manifestación externa de la individualidad corporal no pueden “ser objeto de libre e injustificada disposición y manipulación de terceros”. En fin, ha sostenido la Corte que se trata de “un derecho autónomo que puede ser lesionado junto con los derechos a la intimidad, a la honra, al buen nombre de su titular, y cuyo ejercicio está estrechamente vinculado a la dignidad y libertad de la persona”.

111. También ha sostenido que “[u]na consideración elemental de respeto a la persona y a su dignidad, impiden que las características externas que conforman su fisonomía o impronta y que lo identifican más que cualquiera otro signo externo en su concreta individualidad, puedan ser objeto de libre disposición y manipulación por terceros. De ahí que [...] toda persona tiene derecho a su propia imagen y que, sin su consentimiento, ésta no puede ser injustamente apropiada, publicada, expuesta, reproducida o comercializada por otro”.

) El derecho a la inviolabilidad del domicilio en la jurisprudencia constitucional

112. El derecho a la inviolabilidad del domicilio también ha sido catalogado por la jurisprudencia constitucional como un derecho fundamental autónomo. La Corte ha sostenido que este derecho representa de manera significativa “el principio de separación entre lo

público y lo privado”, en tanto supone, en principio, excluir “la intervención estatal de espacios cerrados al público que se encuentran estrechamente vinculados con el ejercicio libre de la vida privada”.

113. Lograr el objetivo de salvaguardar el domicilio frente intromisiones públicas manifiestas significa a un mismo tiempo la posibilidad de garantizar el principio de libertad en sus distintas expresiones, “tales como el derecho a la intimidad, “esencial en una sociedad democrática respetuosa del valor de la autonomía” , al libre desarrollo de la personalidad, la libertad de creencias y de cultos y a la libre expresión cultural y de ideas.

114. El vínculo que existe entre la protección del domicilio y la libertad explica que la misma garantía de reserva judicial para su limitación se encuentre tanto respecto de la privación de la libertad, como en el acceso al domicilio (artículo 28 de la Constitución) y en el acceso a las comunicaciones privadas (artículo 15 de la Constitución). El domicilio, entendido en un sentido amplio, se constituye así en un espacio excluido de la intervención pública, salvo la presencia de motivos de interés público, previstos en la ley y verificados previamente por una autoridad judicial, salvo en casos excepcionales determinados y delimitados de manera clara por la ley” .

) El derecho al libre desarrollo de la personalidad en la jurisprudencia constitucional

115. Según el artículo 16 de la Constitución Política, las personas tienen derecho “a desarrollar su personalidad sin más limitaciones que los derechos de los demás y el orden jurídico”. La Corte Constitucional ha encuadrado este derecho bajo la cláusula general de libertad. Además, ha sostenido que acorde con esa disposición puede constatarse una estrecha relación entre este derecho y la dignidad humana, definiéndolo como aquel “que le confiere a la persona natural la potestad para decidir autónomamente sobre sus diferentes opciones vitales, dentro de las restricciones mencionadas en el artículo 16. En la sentencia

T-413 de 2017, la Corporación precisó que, dentro del ámbito de protección del derecho al libre desarrollo de la personalidad, se encuentra la posibilidad de determinar el propio modelo de vida y de adquirir una visión de dignidad específica e individual.

116. De ahí que se ampare la facultad de elegir en forma espontánea y, sin presiones, un estilo y plan de vidas propios, lo que, a su turno, exige por parte de las autoridades estatales respetar esa potestad de sentir, pensar y actuar de manera autónoma y “fijar sus opciones de vida acordes con las propias elecciones y anhelos”. Desde esa perspectiva, se construye la identidad personal, lo que comprende la apariencia física, el modelo de vida que se aspira a realizar, tanto como la identidad sexual y de género.

117. La jurisprudencia constitucional ha sostenido igualmente que, de manera correlativa, las autoridades estatales y la sociedad se encuentran obligadas a no interferir en aquellas decisiones que hacen parte de la intimidad de cada persona y que son el resultado del ejercicio autónomo de su libertad, siempre que esta “no afecte derechos de terceros ni los valores y principios del Estado”.

118. Ha destacado, asimismo, que al ejercer ciertas libertades derivadas del libre desarrollo de la personalidad pueden inscribirse dentro del campo de protección del derecho a la intimidad que “hace parte de la esfera o espacio de vida privada no susceptible de la interferencia arbitraria de las demás personas, que al ser considerado un elemento esencial del ser, se concreta en el derecho a poder actuar libremente en la mencionada esfera o núcleo, en ejercicio de la libertad personal y familiar, sin más limitaciones que los derechos de los demás y el ordenamiento jurídico”.

b) El derecho al hábeas data o a la autodeterminación informática en la jurisprudencia constitucional

119. El hábeas data ha sido caracterizado por la Corte Constitucional como un derecho fundamental, cuya principal función consiste en “equilibrar el poder entre el sujeto concernido por el dato y aquel que tiene la capacidad de recolectarlo, almacenarlo, usarlo y transmitirlo”. A partir de una evolución jurisprudencial gradual, la Corte comenzó a subrayar el carácter autónomo de este derecho y a relacionarlo con la paulatina pero constante consolidación del llamado “poder informático” y el eventual manejo “indiscriminado de los denominados datos personales”.

120. Desde la perspectiva descrita, el derecho al hábeas data dejó de ser “una garantía con alcances limitados”, y pasó a convertirse en un derecho fundamental autónomo con amplios contornos de protección. En esa medida, teniendo como punto de partida la cláusula general de libertad contemplada en el artículo 16 superior y también la específica en el manejo de datos prevista en el primer inciso del artículo 15 superior, la jurisprudencia ha reconocido el derecho a la autodeterminación informática.

121. Así, pues, según la sentencia T-729 de 2002 y, de conformidad con jurisprudencia constitucional reiterada, el derecho al hábeas data tiene los siguientes contenidos principales. En primer lugar, les confiere a todas las personas la facultad de “conocer, actualizar y rectificar la información que sobre ellas se haya recogido en bancos de datos y en archivos de entidades públicas y privadas”. En segundo lugar, somete los procesos de recolección, tratamiento y circulación de datos al respeto de la libertad y demás garantías consagradas en la Constitución”. Finalmente, autoriza a su titular para exigir que el “administrador de las bases de datos personales efectúe su labor con sujeción a estrictos límites constitucionales”.

122. Por otra parte, en vista del impulso que ha tomado el fenómeno de la globalización de la información, el legislador estatutario ha regulado el contenido del derecho fundamental al hábeas data en distintas normatividades y ha generado instrumentos e instancias para su debida protección. En este sentido se pueden mencionar las leyes estatutarias 1266 de 2008

y 2157 de 2021, en el ámbito del hábeas data financiero, y la Ley Estatutaria 1581 de 2012, en el régimen general de tratamiento de datos.

123. En pronunciamientos reiterados esta Corporación ha señalado los rasgos característicos del dato personal. Primero, que se trata de “aspectos exclusivos y propios de una persona natural”. Segundo, que en virtud de la visión de conjunto que se logre con el dato y con otros datos, permite identificar en mayor o en menor medida a una persona. Tercero, la propiedad del dato reside, exclusivamente en su titular, circunstancia que no se modifica por el hecho de que se obtenga por un tercero de manera lícita o ilícita. Cuarto, lo referente a la captación, administración y divulgación del dato está sujeto a reglas o principios especiales.

124. Por su parte, la información reservada es aquella que equivale a datos sensibles y del interés exclusivo y excluyente de su titular, puesto que se encuentra relacionada con la protección de sus derechos a la dignidad humana, a la intimidad, al libre ejercicio de la personalidad, para mencionar algunos de los más importantes. El acceso a esta clase de información está vedado a terceros, excepto cuando se trata de una situación excepcional, en la que i) “el dato reservado constituye ‘un elemento probatorio pertinente y conducente dentro de una investigación penal’” y ii) “dicho dato está directamente relacionado con el objeto de la investigación”.

125. En suma, la protección que se desprende del derecho fundamental al hábeas data incluye, de manera especial, que asuntos vinculados al ámbito de privacidad de sus titulares no sean divulgados sin su autorización. Esta garantía ha sido considerada por la Corte Constitucional como una concretización del principio de libertad, que subyace al ejercicio del derecho en mención, y que les brinda a sus titulares la inmunidad indispensable frente a injerencias de terceros o del Estado.

127. El objeto de la Ley Estatutaria 1581 de 2012 radica, más concretamente, en “desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma”.

128. El artículo 2º de la referida ley se ocupó de establecer su ámbito de regulación y especificó que sus principios y disposiciones se aplicarán “a los datos personales registrados en cualquier base de datos que los haga susceptibles de tratamiento por entidades de naturaleza pública o privada”. Dispuso, asimismo, que la ley regirá “el tratamiento de datos personales efectuado en territorio colombiano o cuando al Responsable del Tratamiento o Encargado del Tratamiento no establecido en territorio nacional le sea aplicable la legislación colombiana en virtud de normas y tratados internacionales”. Adicionalmente, señaló los casos en los que no se aplicará el régimen de protección de datos personales que se establece en esa ley, a saber –se destaca–:

a) A las bases de datos o archivos mantenidos en un ámbito exclusivamente personal o doméstico.

Cuando estas bases de datos o archivos vayan a ser suministrados a terceros se deberá, de manera previa, informar al Titular y solicitar su autorización. En este caso los Responsables y Encargados de las bases de datos y archivos quedarán sujetos a las disposiciones contenidas en la presente ley –se destaca–;

b) A las bases de datos y archivos que tengan por finalidad la seguridad y defensa nacional, así como la prevención, detección, monitoreo y control del lavado de activos y el financiamiento del terrorismo;

c) A las Bases de datos que tengan como fin y contengan información de inteligencia y contrainteligencia;

d) A las bases de datos y archivos de información periodística y otros contenidos editoriales;

e) A las bases de datos y archivos regulados por la Ley 1266 de 2008;

f) A las bases de datos y archivos regulados por la Ley 79 de 1993.

PARÁGRAFO. Los principios sobre protección de datos serán aplicables a todas las bases de datos, incluidas las exceptuadas en el presente artículo, con los límites dispuestos en la presente ley y sin reñir con los datos que tienen características de estar amparados por la reserva legal. En el evento que la normatividad especial que regule las bases de datos exceptuadas prevea principios que tengan en consideración la naturaleza especial de datos, los mismos aplicarán de manera concurrente a los previstos en la presente ley.

129. A propósito del párrafo citado cabe resaltar su importancia en el sentido en que –como lo subrayó la Corte Constitucional en la sentencia C-748 de 2011–, al margen de la finalidad que tenga una base de datos, en la medida en que abarque información y datos personales resulta forzoso acatar los principios generales que regulan el tratamiento y protección de datos.

130. A su vez, el artículo 3º prevé un grupo de definiciones importantes, para efectos de la

ley aludida. Otro concepto relevante, definido por la ley estatutaria en comento es el de tratamiento de datos personales. La Corte consideró importante subrayar que la ley de protección de datos personales no cubre única y exclusivamente el tratamiento de datos que se valen de nuevas tecnologías de la información, sino que abarca también las bases de datos manuales. Por eso insistió en que lo que la ley estatutaria buscó fue “que todas las operaciones o conjunto de operaciones con los datos personales quede regulada por las disposiciones de [la ley estatutaria] en mención, con algunas salvedades”. En tal virtud, el tratamiento implica usar, recolectar, almacenar y suprimir “datos personales que se encuentran registrados en cualquier base de datos o archivos por parte de entidades públicas o privadas cuyo procesamiento sea utilizando medios tecnológicos o manuales”.

a) Principio de legalidad en materia de Tratamiento de datos: El Tratamiento a que se refiere la presente ley es una actividad reglada que debe sujetarse a lo establecido en ella y en las demás disposiciones que la desarrollen;

b) Principio de finalidad: El Tratamiento debe obedecer a una finalidad legítima de acuerdo con la Constitución y la Ley, la cual debe ser informada al Titular;

c) Principio de libertad: El Tratamiento sólo puede ejercerse con el consentimiento, previo, expreso e informado del Titular. Los datos personales no podrán ser obtenidos o divulgados sin previa autorización, o en ausencia de mandato legal o judicial que releve el consentimiento;

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

e) Principio de transparencia: En el Tratamiento debe garantizarse el derecho del Titular a obtener del Responsable del Tratamiento o del Encargado del Tratamiento, en cualquier momento y sin restricciones, información acerca de la existencia de datos que le conciernan;

f) Principio de acceso y circulación restringida: El Tratamiento se sujeta a los límites que se derivan de la naturaleza de los datos personales, de las disposiciones de la presente ley y la Constitución. En este sentido, el Tratamiento sólo podrá hacerse por personas autorizadas por el Titular y/o por las personas previstas en la presente ley;

Los datos personales, salvo la información pública, no podrán estar disponibles en Internet u otros medios de divulgación o comunicación masiva, salvo que el acceso sea técnicamente controlable para brindar un conocimiento restringido sólo a los Titulares o terceros autorizados conforme a la presente ley;

g) Principio de seguridad: La información sujeta a Tratamiento por el Responsable del Tratamiento o Encargado del Tratamiento a que se refiere la presente ley, se deberá manejar con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento;

h) Principio de confidencialidad: Todas las personas que intervengan en el Tratamiento de datos personales que no tengan la naturaleza de públicos están obligadas a garantizar la reserva de la información, inclusive después de finalizada su relación con alguna de las labores que comprende el Tratamiento, pudiendo sólo realizar suministro o comunicación de datos personales cuando ello corresponda al desarrollo de las actividades autorizadas en la presente ley y en los términos de esta.

132. En fin, el artículo 4º fija “el contexto axiológico dentro del cual debe moverse, el proceso informático”, que no puede pasar por alto la existencia de un grupo de criterios generales de obligada observancia para “poder afirmar que el proceso de acopio, uso y difusión de datos personales sea constitucionalmente legítimo”. Los principios de la administración de datos personales consignados en esta norma “son oponibles a todos los sujetos involucrados en el tratamiento del dato, entiéndase en la recolección, circulación, uso, almacenamiento, supresión, etc., sin importar la denominación que los sujetos adquieran, es decir, llámense fuente, responsable del tratamiento, operador, encargado del tratamiento o usuario, entre otros” -negritas en el texto citado-.

133. A propósito del artículo 4º mencionado, en la sentencia C-748 de 2011 la Corte advirtió, asimismo, sobre la necesidad de aplicar otros principios que se originan en normas constitucionales, tales como i) “la prohibición de discriminación por las informaciones recaudadas en las bases de datos; ii) el principio de interpretación integral de los derechos constitucionales y iii) la obligación de indemnizar los perjuicios causados por las posibles fallas en el proceso de administración de datos”.

134. En ese mismo horizonte de comprensión, resaltó que a la luz del principio pro-persona al que se acude cuando se trata de fijar el sentido y alcance de las normas constitucionales, la administración de datos personales deberá, en todo caso, subordinarse a la eficacia de los derechos fundamentales. Así mismo, los principios deben entenderse de manera armónica, coordinada y sistemática, respetando, en todo caso, los contenidos básicos del derecho fundamental al hábeas data.

135. Además, observó que existía un conjunto de directrices no enlistadas en el artículo 4º que también deben ser tomadas en cuenta al momento de realizar una lectura sistemática de la ley en comento. Entre estas, mencionó las siguientes: a) aun cuando la ley exceptúa

algunas materias del régimen general de la administración de datos, no las excluye y este tema debe abordarse teniendo en cuenta el principio de proporcionalidad, respondiendo, a su vez, a los estándares internacionales de protección; b) en el marco de la estructura estatal debe existir un órgano encargado de garantizar los principios en términos de imparcialidad e independencia; c) debe presentarse una equivalencia de estándares de protección para la transferencia internacional de datos, pues, como se deduce del artículo 26 del Proyecto de Ley Estatutaria, hay una prohibición de transferencia internacional a cualquier tipo de países que no proporcionen niveles adecuados de protección de datos.

136. De otro lado, el artículo 5º de la Ley Estatutaria 1581 de 2012 se refiere a los datos sensibles como “aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación”. Entre este tipo de datos, la norma mencionó los “que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual y los datos biométricos”.

137. La Corte Constitucional, al ejercer el control automático en relación con el artículo 5º de la Ley Estatutaria de 2012, trajo a colación que de acuerdo con lo resuelto en la sentencia C-1011 de 2008, la información sensible podía considerarse como aquella relacionada con aspectos directamente vinculados con el núcleo esencial del derecho a la intimidad, entendido este como aquel que le asegura a las personas una “esfera o espacio de vida privada no susceptible de la interferencia arbitraria de las demás personas, que al ser considerado un elemento esencial del ser, se concreta en el derecho a poder actuar libremente en la mencionada esfera o núcleo, en ejercicio de la libertad personal y familiar, sin más limitaciones que los derechos de los demás y el ordenamiento jurídico”.

138. Con todo, la Corte resaltó que el listado contemplado en el artículo 5º en mención no

era taxativo, “sino meramente enunciativo de datos sensibles, pues los datos que pertenecen a la esfera íntima son determinados por los cambios y el desarrollo histórico”.

139. El artículo 6º de la Ley Estatutaria 1581 de 2012 prohibió el tratamiento de datos sensibles y relacionó un conjunto de salvedades entre las que se encuentran las siguientes:

a) El Titular haya dado su autorización explícita a dicho Tratamiento, salvo en los casos que por ley no sea requerido el otorgamiento de dicha autorización;

b) El Tratamiento sea necesario para salvaguardar el interés vital del Titular y este se encuentre física o jurídicamente incapacitado. En estos eventos, los representantes legales deberán otorgar su autorización;

c) El Tratamiento sea efectuado en el curso de las actividades legítimas y con las debidas garantías por parte de una fundación, ONG, asociación o cualquier otro organismo sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, siempre que se refieran exclusivamente a sus miembros o a las personas que mantengan contactos regulares por razón de su finalidad. En estos eventos, los datos no se podrán suministrar a terceros sin la autorización del Titular;

d) El Tratamiento se refiera a datos que sean necesarios para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial;

e) El Tratamiento tenga una finalidad histórica, estadística o científica. En este evento deberán adoptarse las medidas conducentes a la supresión de identidad de los Titulares.

140. Cuando ejerció el control de constitucionalidad de la Ley Estatutaria en comento, la Corte puso de presente que prohibir el tratamiento de datos sensibles comporta una garantía que contribuye a materializar los derechos fundamentales al hábeas data y a la intimidad, estrechamente unidos a la protección de la dignidad humana. No obstante, también precisó que, ocasionalmente, el tratamiento de datos resulta necesario para prestar adecuadamente servicios.

141. Para ilustrar su aserto trajo a colación el servicio de atención médica y de educación. Mencionó, igualmente, la realización de derechos ligados precisamente a la esfera íntima de las personas –como la libertad de asociación y el ejercicio de las libertades religiosas y de opinión– y advirtió que las “excepciones del artículo 6 responden precisamente a la necesidad del tratamiento de datos sensible en dichos escenarios”.

142. Además, puntualizó que, tratándose de casos exceptuados, se generan riesgos altos para la preservación del derecho de hábeas data, intimidad y dignidad de quienes son titulares de los datos. En estos casos, quienes agencian los datos asumen una responsabilidad reforzada, en el sentido de que no solo deben cumplir con los principios previstos en el artículo 4º, sino también los deberes consignados en el título VI de la ley en comento. Esta exigencia mayor de diligencia se aplica también en materia sancionatoria administrativa y penal.

143. En fin, la regulación del derecho fundamental al hábeas data en la Ley Estatutaria de Protección de Datos Personales procura responder al actual desarrollo de las tecnologías de información, que, como recuerda la doctrina, permite hoy por hoy recopilar y guardar, sin límite espacial alguno, un conjunto enorme de datos sobre las personas, catalogar esa información e interrelacionarla con los demás datos que sobre ellas se tengan, sin perjuicio de que hayan sido resguardadas en archivos diferentes, relativos a distintas épocas de su

existencia y tras haber sido recopiladas, incluso, en lugares diversos. Dicho en pocas palabras, actualmente la posibilidad de acumular y recabar información resulta inmensa. Esto puede suceder en segundos, al margen del lugar en el que las personas se encuentren.

145. En tal caso, bastaría con examinar los principios “de libertad, necesidad, veracidad, integridad, finalidad, así como su relevancia en la materialización del derecho fundamental al hábeas data, en la protección de datos personales y en la autodeterminación informática. Más adelante, cuando se analice la disposición acusada, la Sala hará una exposición de los problemas que en la práctica enfrenta la aplicación de la regulación vigente con graves repercusiones para los derechos fundamentales afectados, especialmente en el campo de aplicación de los sistemas de videovigilancia y seguridad.

7. Fronteras constitucionales y legales a las que se sujeta la Policía Nacional en su rol de Policía Judicial

146. Según el artículo 218 superior, la Policía Nacional es un cuerpo armado permanente de naturaleza civil que busca mantener las condiciones indispensables para el ejercicio de los derechos y libertades públicas. La norma agrega que, con su tarea, esta autoridad busca asegurar la convivencia pacífica de quienes habitan el territorio nacional.

147. Desde muy temprano, la Corte Constitucional se pronunció sobre la función que cumple la Policía Nacional en materia de orden público. Ahora bien, lejos de describir el orden público como un valor en sí mismo, la Corporación lo denotó como “el conjunto de condiciones de seguridad, tranquilidad y salubridad que permiten la prosperidad general y el goce de los derechos humanos”. Desde esa perspectiva, resulta claro que la garantía de estos derechos se convierte en condición de posibilidad y freno del poder que le atribuyó el ordenamiento a

la Policía Nacional.

148. Además, en distintos pronunciamientos la Corte ha sostenido que la función atribuida a la policía “es esencialmente preventiva”. Bajo esa óptica, su tarea consiste, principalmente, en adoptar de manera oportuna y eficaz medidas que aseguren el ejercicio pleno y efectivo de las garantías constitucionales. De este modo, contribuye a la convivencia pacífica en comunidad y con la sociedad.

149. Esta dimensión preventiva que se resalta armoniza con la noción de seguridad ciudadana interpretada en términos de seguridad humana. Así, el sentido y alcance de las funciones atribuidas a la Policía Nacional no pueden separarse de esta noción que resignifica el concepto tradicional de orden público. De todos modos, esta Corte ha reiterado, de manera constante, que la Policía Nacional debe sujetarse en el ejercicio de sus funciones a unos lineamientos mínimos de orden superior. Entre estos, pueden mencionarse los siguientes que revisten importancia para resolver el asunto bajo examen:

Primero, se encuentra sometida al principio de legalidad, pues hay facetas en el ejercicio de sus funciones que pueden implicar el desconocimiento de los derechos fundamentales y las libertades públicas.

Segundo, debe someterse al principio de necesidad, en el sentido de que, para conservar y preservar el orden público, únicamente, puede adoptar aquellas medidas imprescindibles y eficaces.

Tercero, se sujeta a los principios de proporcionalidad y razonabilidad, tomando en cuenta las circunstancias y el fin que se pretende alcanzar.

Cuarto, debe hacer efectivas las tareas que le confía el ordenamiento en concordancia con el principio de igualdad de los ciudadanos ante la ley, lo que implica, simultáneamente, que debe proscribir las discriminaciones injustificadas en el sentido previsto por el artículo 13 superior.

a. a) Funciones que el ordenamiento le confiere a la Policía Nacional en su rol de Policía Judicial y sus límites

150. El ordenamiento también le confiere a la Policía Nacional atribuciones de Policía Judicial. Esto se desprende de lo establecido en el numeral 5º del artículo 251 de la Carta Política a cuyo tenor, en el ejercicio de sus funciones, la Fiscalía General de la Nación podrá –se destaca–:

5. Otorgar, atribuciones transitorias a entes públicos que puedan cumplir funciones de Policía Judicial, bajo la responsabilidad y dependencia funcional de la Fiscalía General de la Nación.

151. Si bien existen otras autoridades facultadas por el ordenamiento para ejercer funciones de Policía Judicial, tales como la Procuraduría General de la Nación, la Contraloría General de la República y aquellas previstas en los artículos 202 y 203 de la Ley 906 de 2004, el artículo 48 de la Ley 2197 de 2022 acusado en el expediente de la referencia se refirió, en concreto, a la Policía Nacional. Con todo, el artículo 201 del Código de Procedimiento Penal es muy claro en que solo las dependencias especializadas de la Policía Nacional se encuentran capacitadas para el efecto y “no toda la Policía Nacional”. Lo anterior, sin perjuicio de lo dispuesto en el párrafo 1º de esa misma disposición, según el cual “[e]n los lugares del territorio nacional donde no hubiere miembros de Policía Judicial de la Policía Nacional, estas funciones las podrá ejercer la Policía Nacional” –se destaca–.

153. De ahí que el ejercicio de esta potestad no pueda efectuarse para propósitos distintos a los previstos en el ordenamiento jurídico –se destaca. Si ello no fuera así, se estaría ante “un problema de desviación de poder e, incluso, ante el delito de abuso de autoridad por parte del funcionario o la autoridad administrativa”. En la oportunidad traída a colación en la sentencia referida la Corte sostuvo que no desconocía “la aguda situación delincuencia que vive el país”, sin embargo, advirtió que tampoco podía pasarse por alto la crítica situación de derechos humanos que ha conocido el país en los últimos años”.

154. Sobre las facultades de la Policía Nacional como Policía Judicial también se pronunció la Corte Constitucional en la sentencia C- 594 del 2014. Previamente realizó un conjunto de consideraciones sobre la Policía Judicial, en general, y distinguió dos acepciones. La primera orgánica y la segunda funcional. En la referida sentencia la Sala Plena resaltó que, si bien el rol de policía judicial no es el propio ni el característico de la Policía Nacional, los integrantes de esta institución “en sus dependencias especializadas [pueden] ser investidos de tal función o supletoriamente la [tienen] que ejercer, lo cual es ocasional y excepcional” –se destaca–.

155. Se reitera: en lo que hace concretamente a la Policía Nacional, la Corte insistió en que, pese a la naturaleza investigativa de la función que se le atribuye a esta autoridad como Policía Judicial, tal actividad se debe adelantar bajo la dirección y coordinación de la Fiscalía General de la Nación. El alcance de esta atribución dependerá siempre de lo que establezca la ley en relación con cada etapa del proceso, pero se centra en comprobar los hechos y las circunstancias para el juzgamiento.

156. A su turno, el artículo 33 de la Ley 270 de 1996 se refirió a la dirección, coordinación y control de las funciones de Policía Judicial. Es de anotar, que la disposición prevista en el

artículo 33 de la Ley 270 de 1996 fue objeto de control automático de constitucionalidad y declarado exequible por esta Corporación mediante la sentencia C-037 de 1996. En aquella ocasión, la Corte hizo hincapié en que, acorde con las normas constitucionales, el Estado ejerce el monopolio de la acción penal y esto sucede por conducto de la Fiscalía General de la Nación. Con todo, este monopolio ya no existe, puesto que fue modificado por el Acto Legislativo 06 de 2011. El parágrafo segundo del actual artículo 250 de la Carta Política establece que “[atendiendo la naturaleza del bien jurídico o la menor lesividad de la conducta punible, el legislador podrá asignarle el ejercicio de la acción penal a la víctima o a otras autoridades distintas a la Fiscalía General de la Nación. En todo caso, la fiscalía General de la Nación podrá actuar en forma preferente.

b) Medidas que restrinjan derechos fundamentales requieren autorización judicial previa

157. Con ocasión de la sentencia C-336 de 2007, la Corporación precisó que de lo consignado en el artículo 250 superior se desprendía la voluntad del Constituyente encaminada a “radicar en cabeza de los jueces de control de garantías la adopción de las medidas necesarias para asegurar la comparecencia de los imputados al proceso penal”. La Corte expresó que sólo excepcionalmente y previa regulación legal que incluya los límites y eventos en que procede, la Fiscalía podría “efectuar capturas”; “adelantar directamente registros, allanamientos, incautaciones e interceptación de comunicaciones, sometidos al control posterior del juez de control de garantías”. Subrayó que “en todos los demás eventos en que, para el aseguramiento de los elementos materiales probatorios, se requiera medidas adicionales que impliquen afectación de derechos fundamentales deberá mediar autorización (es decir, control previo) por parte del juez de control de garantías” –se destaca–.

158. En suma, la Corte Constitucional resaltó que la limitación de los derechos fundamentales tiene “por regla general reserva judicial, por lo cual los registros domiciliarios y las privaciones de libertad cuando se efectúan por autoridades policiales deben tener sustento en una orden judicial” –se destaca–.

159. A propósito de medidas relacionadas con labores de vigilancia y seguimiento, la jurisprudencia constitucional también las ha acotado y las ha relacionado con aquellas adelantadas en el marco de investigaciones seguidas por la Fiscalía General de la Nación en las que actúa la Policía Judicial para obtener y asegurar las pruebas de una conducta punible. Ha destacado que se trata de figuras ampliamente aceptadas en el derecho comparado y ha dicho, asimismo, que se encuentran constitucionalmente legitimadas, puesto que persiguen una finalidad compatible con la Carta Política cual es la de perseguir y sancionar conductas que menoscaban bienes jurídicamente tutelados.

160. No obstante, ha subrayado que tales medidas no son ilimitadas, sino que tienen un alcance específico “respecto de eventos que no afecten el núcleo esencial del derecho fundamental a la intimidad como campos abiertos, a plena vista, o cuando se hayan abandonado objetos, por lo cual no se podrá aplicar en aquellos casos en los cuales sea necesaria una afectación más profunda de la intimidad como allanamientos y registros, interceptaciones o retenciones” -de destaca-.

161. De otra parte, la jurisprudencia constitucional ha sostenido que la finalidad de la medida debe encontrarse definida en la norma de manera directa, clara y específica. Además, debe tener una relación con la indagación que adelanta la Fiscalía General de la Nación en el marco de una investigación existente. La medida no solo debe ser apta o idónea para recaudar la información sobre la conducta punible, sino debe ser igualmente necesaria, esto es, constituir el medio menos restrictivo del derecho fundamental en juego. Por último, debe ser proporcional en sentido estricto -se destaca-.

162. En síntesis, la jurisprudencia ha sido consistente y reiterada en precisar que, con el objeto de desarrollar actividades encaminadas a obtener elementos materiales probatorios o evidencia física para esclarecer un hecho presuntamente delictivo, cualquier afectación a los

derechos fundamentales de las personas está encomendada a una autoridad judicial, la que debe verificar que esta facultad se ejerza de manera idónea, necesaria y proporcional –se destaca–.

163. Por consiguiente, las dependencias especializadas de la Policía Nacional a quienes se atribuye la facultad de Policía Judicial y, en su ausencia, la Policía Nacional deben sujetarse de manera estricta a las exigencias previstas en el ordenamiento, entre las que se cuenta que, según lo dispuesto en el numeral 3º del artículo 250 superior, obtengan autorización judicial previa cuando las acciones de investigación afecten derechos fundamentales, tales como los derechos a la intimidad y al hábeas data. No obstante, como se verá esa autorización podrá ser posterior tratándose de casos de flagrancia –se destaca–.

c) La autorización judicial en casos de flagrancia o actos urgentes puede ser posterior

164. Como se expuso, la Corte ha reiterado de manera constante y consistente, que las autoridades judiciales son garantes de los derechos fundamentales en el ordenamiento constitucional. Lo anterior, en tanto “el rol del control judicial en estas materias realiza los postulados mismos del Estado de Derecho, particularmente la exclusión de la arbitrariedad y el sometimiento del poder público al ordenamiento jurídico y convierte al juez en pieza protagónica de la protección de la libertad” .

166. En la sentencia C-879 de 2011, la Corte afirmó que la flagrancia podía describirse como

una situación actual que torna imperiosa la actuación inmediata de las autoridades [o de los particulares], cuya respuesta pronta y urgente impide la obtención previa de la orden judicial

para allanar y la concurrencia del fiscal a quien, en las circunstancias anotadas, no podría exigírsele que esté presente, ya que de tenerse su presencia por obligatoria el aviso que debería cursársele impediría actuar con la celeridad e inmediatez que las situaciones de flagrancia requieren, permitiendo, de ese modo, la reprochable culminación de una conducta delictiva que pudo haber sido suspendida merced a la penetración oportuna de la autoridad al lugar en donde se desarrollaba(...).

De esta forma, la flagrancia está determinada por la proximidad viva al hecho delictivo en cuanto tal, lo cual genera una autorización a quien fuera, particular o autoridad, para capturar al que lo comete, lo ha cometido, o existen ciertas, claras y objetivas razones para creer que así lo es o lo fue. Lo anterior, de acuerdo con la jurisprudencia de la Sala Penal de la Corte Suprema de Justicia, donde se ha dicho que la expresión flagrancia viene de ‘flagrar’ que significa arder, resplandecer, y que, en el campo del derecho penal, se toma en sentido metafórico, como el hecho que todavía arde o resplandece, es decir que aún es actual.

167. En general, la jurisprudencia constitucional ha reiterado que cuando se está ante circunstancias urgentes e inminentes que exigen una reacción inmediata, oportuna y eficiente de las autoridades o de los particulares para evitar que la tarea de perseguir y atribuir responsabilidad a quien ha cometido un delito pueda verse truncada, la autorización judicial puede tener lugar de manera posterior –se destaca–.

168. En el caso que ocupa la atención de la Sala resulta central lo establecido en el artículo 301.4 de la Ley 906 de 2004, esto es, que entre los supuestos que se pueden caracterizar como flagrancia se encuentra la situación de aquellas personas que fueron “sorprendidas o individualizadas en espacios abiertos al público con el apoyo de una grabación mediante dispositivo de video y son aprehendidas inmediatamente después. Ese mismo calificativo lo aplica la norma en mención a las grabaciones de video que se llevan a cabo en lugares privados bajo la condición de que estas hayan sido previamente consentidas por la persona o personas que residen en estos espacios –se destaca–.

169. Adicionalmente, es importante tener en cuenta lo previsto en el artículo 205 de la misma ley que se refiere a la actividad de la Policía Judicial en la indagación e investigación. En el artículo mencionado se describen los denominados actos urgentes que deben desarrollar quienes ejercen funciones de Policía Judicial en la indagación e investigación -se destaca-. La Corte ha señalado que en eventos como estos estaría justificado encausar la investigación penal y determinar la pertinencia de efectuar actos urgentes, incluso, antes de que se disponga la apertura formal de una investigación.

170. Por tanto, cuando las dependencias especializadas de la Policía Nacional -o la Policía Nacional en aquellos lugares del territorio estatal en los que no existan tales dependencias especializadas-, conozcan de actos urgentes a los que se refiere el artículo 205 citado, deberán reportar la iniciación de estas actuaciones a la Fiscalía y realizar las tareas a las que haya lugar sin que sea necesario que medie orden judicial. Lo anterior, por cuanto estas actividades están dirigidas a evitar que se pierdan o alteren elementos materiales de convicción o evidencia física, tales como inspecciones en el lugar de los hechos, inspección de cadáver, entrevistas, interrogatorios derivados del conocimiento de los hechos con fundamento en una noticia criminal (fuentes formales e informales) .

171. Para el asunto que se analiza en la presente ocasión reviste especial importancia que, acorde con la jurisprudencia sentada por la Corte Constitucional, aquellos videos que sean requeridos a personas o a empresas privadas que puedan afectar negativamente su esfera personal, pueden ser solicitados, pero debe mediar el consentimiento del titular de la información. Es de resaltar que la necesidad de consentimiento previo del titular de la información que consta en los videos también se aplica a aquellos que registran información en espacios semipúblicos o semiprivadas como supermercados, colegios, iglesias, comercios, entre otros.

172. Con todo, si la solicitud es respondida de manera negativa, las autoridades respectivas deberán redactar un acta en la que conste que los videos serán conservados mientras se obtiene la orden judicial. Lo anterior, con el fin de preservar la evidencia que permitirá esclarecer un hecho punible. Tratándose de videos que sean captados en el espacio público y, no afecten la intimidad de las personas, pueden solicitarse sin la necesidad de que medie orden judicial. De todas maneras, los registrados en el espacio público o en instituciones públicas que no afecten la intimidad de las personas, pueden solicitarse sin orden judicial.

173. En relación con los aspectos expuestos, se debe hacer hincapié, una vez más, en que las actividades o actuaciones relacionadas con allanamientos, retención de correspondencia, interceptación de comunicaciones, recuperación de información producto de transmisión de datos a través de redes de comunicaciones, registros a equipos electrónicos o dispositivos de almacenamiento, vigilancia y seguimiento de personas, vigilancia de cosas, actuación de agente encubierto, entrega vigilada, capturas, búsqueda selectiva en bases de datos, una vez finalizadas, una vez finalizadas, deben ser comunicadas a más tardar dentro de las 12 horas siguientes, mediante informe realizado por la autoridad de policía judicial al fiscal del caso, a efectos de que este, dentro de las 24 horas siguientes al recibido, comparezca ante el juez con función de control de garantía para solicitar su legalidad” –se destaca–.

174. A partir de los pronunciamientos efectuados por esta Corporación, en particular, el realizado en la sentencia C-014 de 2018, puede concluirse que “el Juez de Garantías ejerce, por lo general, un control previo de todas las diligencias de investigación penal que limitan los derechos fundamentales, salvo las intervenciones a la intimidad contenidas en el artículo 250.2. C.P., cuya revisión de legalidad es posterior y se ejerce tanto sobre el contenido de la orden como en cuanto a su ejecución”. En todo caso, la jurisprudencia constitucional ha puesto un énfasis central en que, a partir de la entrada en vigor del sistema penal acusatorio, incorporado a nuestro ordenamiento por medio del Acto Legislativo 03 de 2002 y, desarrollado por la Ley 906 de 2004,

la labor de protección a la intimidad y los demás derechos de los afectados con los procedimientos policiales de investigación fue conferida al “Juez de Control de Garantías”. Concebido como una salvaguarda para los derechos de las partes y, en especial, del procesado, el Juez de Garantías responde al principio de necesidad de supervisar el respeto por las garantías constitucionales en el marco de un eficaz desenvolvimiento de las investigaciones, del propósito de conjurar excesos y medidas desproporcionadas, irrazonables e innecesarias y de dotar de corrección sustantiva el procedimiento.

175. Por consiguiente, en la medida en que las autoridades correspondientes ordenen realizar procedimientos que puedan afectar negativamente los derechos fundamentales a la intimidad o al hábeas data, el control judicial posterior se encaminará a verificar si, tanto la orden emitida, como la práctica y, los resultados de las diligencias se ajustan al principio de legalidad. El término constitucional de treinta y seis (36) horas para adelantar ese control comenzará a contabilizarse tras la finalización de la ejecución de los procedimientos ordenados.

8. El papel de las empresas privadas de seguridad y vigilancia. Alcance y límites. Reiteración de jurisprudencia

176. Las empresas de vigilancia y seguridad privada se encuentran autorizadas y reguladas mediante el Decreto ley 356 de 1994, que en su artículo 2º definió este servicio como:

las actividades que en forma remunerada o en beneficio de una organización pública o privada, desarrollan las personas naturales o jurídicas, tendientes a prevenir o detener perturbaciones a la seguridad y tranquilidad individual en lo relacionado con la vida y los bienes propios o de terceros y la fabricación, instalación, comercialización y utilización de equipos para vigilancia y seguridad privada, blindajes y transportes con este mismo fin.

177. En su artículo 3º agregó que los servicios de que trata el precepto referido solo “podrán prestarse mediante la obtención de licencia o credencial expedida por la Superintendencia de Vigilancia y Seguridad Privada, con base en potestad discrecional, orientada a proteger la seguridad ciudadana”. Adicionalmente, dispuso que la mencionada Superintendencia podrá suspender o cancelar la licencia o credencial expedida, con fundamento en esa potestad discrecional.

178. En la sentencia C-128 de 2018, la Corte recordó que, el artículo 216 superior incorporó el principio de exclusividad de la fuerza pública, de ahí que existen atribuciones –como las relacionadas con la preservación del orden público–, que son de uso exclusivo de la Policía Nacional y, de manera alguna, pueden ser atribuidas a particulares. Advirtió, asimismo, que el Estado no estaba autorizado a conferir a los particulares la facultad de detentar la posesión o usar armas que pongan en entredicho “la naturaleza exclusiva de la Fuerza Pública”.

179. La directriz mencionada comporta que al legislador le está vedado promover o proteger la presencia de organismos armados no oficiales o de naturaleza privada que pretendan cumplir de modo paralelo con las tareas que la Constitución les confió, en exclusivo, a las fuerzas militares y a la Policía Nacional.

180. A propósito de este aspecto, resulta preciso advertir que la jurisprudencia constitucional, inicialmente, puso énfasis en el deber de solidaridad previsto en el artículo 95 para justificar la participación de los particulares en la prestación del servicio de seguridad y vigilancia ciudadana. Esta postura fue modificada por la propia Corte Constitucional en la sentencia C-251 de 2002. En aquella ocasión consideró que previamente había dejado de lado “el principio de exclusividad de la fuerza pública”. En tal virtud, encontró que no era factible atribuir “a los particulares funciones propias del mantenimiento del orden público o la

participación en los conflictos armados”. Desde esa óptica, puntualizó que el deber de solidaridad no podía envolver la facultad de “asignar a los particulares funciones vinculadas al uso de la fuerza armada o a la inteligencia” -se destaca-.

181. A su turno, en la sentencia C-995 de 2004, la Corte precisó que la seguridad es un servicio público y que “la vigilancia y seguridad a la que hacía referencia el Decreto ley 356 de 1994 era la seguridad ciudadana ordinaria no asociada al conflicto armado”. Con todo, la Corte fue enfática en afirmar que “ningún servicio de vigilancia privada puede desplazar o sustituir la actividad de defensa y seguridad desplegada por las fuerzas armadas del Estado”, tanto como fue contundente en advertir que estos “servicios de seguridad privados se adelantarán siempre en los términos del régimen legal vigente y dentro del pleno respeto a la Constitución” -se destaca-.

182. Estas posturas han sido reiteradas también en sede de tutela. En las sentencias T-909 de 2011 y T-030 de 2017, la Corte enfatizó que la tarea asignada a las empresas de vigilancia y seguridad privadas consiste en prevenir y disuadir conductas tendientes a “configurar la comisión de un delito o que atenten contra los bienes que son dispuestos para su protección”. Ahora, la jurisprudencia constitucional también ha señalado que la función atribuida a estas empresas no las exime de “respetar y garantizar los derechos fundamentales y las libertades de la comunidad en general” -se destaca.

183. Respecto de las medidas que podrían adoptar las empresas de seguridad privada en el ejercicio de sus funciones, la Corte ha insistido en que, con el objeto central de contribuir a mantener el orden público, facilitar la convivencia y respetar los derechos fundamentales estas empresas estarían facultadas a usar medidas razonables, lo que, en todo caso, excluye habilitarlas para que hagan cumplir normas de policía, toda vez que esta tarea “está reservada a los funcionarios investidos de autoridad”.

184. En relación con las condiciones a las que se sujeta el funcionamiento de empresas que prestan el servicio de vigilancia y seguridad, ha dicho la Corte que estas deben observar las siguientes –se mantienen las notas a pie de página en el texto citado–:

(a) su creación y funcionamiento debe estar regulado por el legislador y bajo la estricta inspección, vigilancia y control del Gobierno; (b) su objeto es la protección de la seguridad de la propiedad y de las personas, sin que ello involucre en modo alguno el ejercicio de actividades de conservación del orden público, funciones de inteligencia, ni mucho menos aquellas tareas vinculadas al conflicto armado.

185. Adicionalmente, la Corte ha reiterado que las funciones prestadas por empresas de vigilancia y seguridad privada no pueden ser intrusivas y deben cumplir un conjunto de exigencias para evitar que desconozcan el principio de exclusividad de la fuerza pública. Estos requerimientos son –se mantienen las notas a pie de página en el texto citado–:

(i) que no usen armas de uso exclusivo de la Policía Nacional, (ii) que su objetivo no sea el de defender una comunidad, ni restablecer el orden público, ni generar las condiciones para el ejercicio pleno de los derechos y libertades –tareas de competencia exclusiva a la fuerza pública, sino el de la protección de bienes o de personas que específicamente requieren de este servicio, (iii) que no se trate de admitir el ejercicio de la fuerza por parte de particulares, en situaciones en las cuales existe un conflicto social o político previo, cuya solución pretenda lograrse por medio de las armas, (iv) que la autorización para utilizar armas no desplace la función de la fuerza pública y (v) que se ejerza el poder de vigilancia y supervisión del Estado previsto para las armas de uso civil.

186. Como se señaló, en Colombia la actividad especializada de vigilancia y seguridad privada está regulada por el Decreto ley 356 de 1994. Este estatuto incorpora normas de tipo organizacional, operacional y técnico. Al respecto esta Corte ha sostenido que los preceptos allí consignados se dirigen a normar “la seguridad ciudadana ordinaria, no asociada al

conflicto armado”. Así, su objetivo principal se centra en regular “ciertas actividades realizadas por los particulares, dirigidas a disminuir los riesgos personales que puedan amenazar la vida, la integridad física o los bienes de las personas”. Tareas estas que se encuentran sujetas al control de la Superintendencia de Vigilancia y Seguridad Privada.

187. En suma, si bien la jurisprudencia constitucional ha reconocido que el servicio de seguridad y vigilancia privada no riñe, ni puede interferir, con el servicio público de policía, igualmente ha sido clara en afirmar que “la ley no puede delegar o transferir a los particulares la función pública que consiste en el mantenimiento de las condiciones necesarias para el ejercicio de los derechos y libertades públicas o el aseguramiento de la paz, es decir, la conservación del orden público interno”. El logro de este propósito central fue atribuido de manera exclusiva a la fuerza pública, esto es, se encuentra en manos del Ejército y de la Policía Nacional.

9. Tecnología relacionada con circuitos cerrados de vigilancia y seguridad privada

188. Los circuitos cerrados de vigilancia y seguridad privada son sistemas televisivos que exhiben unas características propias, pues tienen un acceso limitado. La Corte Constitucional no ha sido ajena a esta temática. En las sentencias T-114 de 2018 y T-094 de 2020 la Corporación precisó que se trataba de “un conjunto de componentes directamente entrelazados, [integrado por] una o varias cámaras de vigilancia conectadas a uno o más monitores o televisores, los cuales reproducen imágenes capturadas que crean un circuito de imágenes”.

189. Resulta indispensable destacar que las cámaras de circuitos cerrados de vigilancia y seguridad privada captan, entre otras, información privada y personalísima –se destaca-. Tal circunstancia ha sido especialmente resaltada por la Corte Constitucional en las sentencias mencionadas. En estas se afirmó que existe la posibilidad de que las cámaras de vigilancia –así estén ubicadas en lugares públicos-, capten información “semiprivada, privada o

reservada, por lo que permitir su libre acceso podría contravenir los postulados de la Constitución y la Ley 1581 de 2012". Además, la Corte ha citado la Guía para la Protección de Datos Personales en Sistemas de Videovigilancia expedida por la Superintendencia de Industria y Comercio, en donde se afirma que los sistemas de videovigilancia son intrusivos de la privacidad, como más adelante se verá en detalle –se destaca–.

190. La Corporación también ha indicado que las imágenes pueden quedar almacenadas en medios analógicos o digitales, según lo requiera el usuario. Como lo advirtió en la sentencia T-114 de 2018, videos captados por esos sistemas pueden contener información cuya divulgación se encuentra sujeta a restricciones –se destaca–. De otra parte, es importante resaltar que las empresas de seguridad y vigilancia privadas que instalan estos medios tecnológicos deben estar previamente autorizadas. En ese sentido, considera la Sala importante indagar por el fenómeno de los sistemas cerrados de vigilancia y seguridad privada y su marco jurídico.

a. a) El fenómeno de la videovigilancia mediante circuitos cerrados de vigilancia y seguridad privada y su marco jurídico

191. Una mirada a conjuntos residenciales, casas y edificios privados, sedes de empresas, instituciones, colegios, universidades, centros comerciales muestra que el fenómeno de los sistemas cerrados de seguridad y vigilancia a cargo de empresas privadas es una tendencia creciente. Son diversas las razones que se esgrimen para justificar esta práctica. Principalmente, se aducen motivos de seguridad de bienes y personas en lugares específicos, pues se estima que tales sistemas resultan idóneos para monitorear y observar actividades en diferentes espacios con efectos preventivos y disuasorios. Si se considera que acciones delictivas también pueden quedar, eventualmente, captadas por tales sistemas, igualmente se acude a estos con el propósito de usar las imágenes registradas como evidencia para fines de judicialización.

192. Es importante resaltar que los datos personales se relacionan, en este caso, con personas físicas “identificadas o inidentificables”. Tratándose de aquellos sistemas que se traducen en imágenes y sonido, de todas maneras, se consideran datos personales, al margen de si se usan en un circuito cerrado o si no se relacionan con datos personales del interesado o corresponden a personas cuyos rostros no han sido filmados o contienen otra información captada a través de la videovigilancia.

193. En Colombia resulta aplicable a la recolección de imágenes por medio de sistemas de videovigilancia en las que queden vinculadas personas determinadas o indeterminadas la Ley Estatutaria 1581 de 2012 a la que se hizo mención en precedencia. De otra parte, como ya se indicó, rige la Guía de Protección de Datos Personales en Sistemas de Videovigilancia expedida por la Superintendencia de Industria y Comercio. Dada su importancia para examinar la constitucionalidad de la disposición acusada, la Sala se referirá en extenso al contenido del aludido documento.

b) Guía para la Protección de Datos Personales en Sistemas de Videovigilancia expedida por la Superintendencia de Industria y Comercio

194. El 16 de septiembre de 2016, la Superintendencia de Industria y Comercio hizo pública la Guía para la Protección de Datos Personales en Sistemas de Videovigilancia y recordó que esta tecnología busca “garantizar la seguridad de bienes o personas”. Además, destacó que su uso se ha incrementado, pues se consideran instrumentos idóneos “para realizar el monitoreo y la observación de actividades en escenarios domésticos, empresariales, laborales y públicos”.

195. El documento precisó que la actividad de monitoreo y observación que se lleva a cabo

por medio de los sistemas de video vigilancia y seguridad privada da paso a recopilar imágenes de personas y, en este sentido, efectúa un manejo de datos personales, acorde con la definición prevista en el literal c) del artículo 3 de la Ley 1581 de 2012 -se destaca-. De tal forma, el tratamiento de estos datos debe sujetarse a la plena observancia de los principios consignados en la referida ley estatutaria, mencionados líneas atrás.

196. Así mismo, advirtió acerca de que los sistemas de videovigilancia han sido considerados “como intrusivos de la privacidad al involucrar herramientas como el monitoreo y la observación de las actividades que realizan las personas a lo largo del día” -se destaca-. Es por esto, por lo que la Guía llama la atención acerca de la importancia de tomar en cuenta si, en efecto, resulta necesario usarlos y evaluar si ese requerimiento se satisface con su implementación o si hay otros instrumentos que puedan ser usados que generen un impacto menor “en la privacidad de las personas” -se destaca-.

197. La anterior advertencia muestra el vínculo directo existente entre la aludida exigencia y el principio de finalidad que gobierna el tratamiento de datos personales relacionados con esta tecnología. De ahí se deriva que el fin propuesto con el tratamiento debe ser constitucional y legalmente legítimo y ha de lograr un objetivo “específico, explícito e informado” -se destaca. Además, señala que acorde con la jurisprudencia constitucional y los estándares internacionales -se destaca-.

el principio de finalidad implica i) un ámbito temporal, es decir, que el periodo de conservación de los datos personales no exceda del necesario para alcanzar la finalidad para la cual se han recolectado, y ii) un ámbito material, que exige que los datos recaudados sean solo los necesarios para cumplir las finalidades perseguidas, lo que implica que los mismos se limiten a los que resulten adecuados, pertinentes y acordes con las finalidades para las cuales fueron recolectados.

198. Bajo esa perspectiva, la información que se recaude únicamente podrá ser usada para el propósito previamente determinado –se destaca-. Si la finalidad de su uso cambia, es complementada o se suprime, entonces resulta indispensable pedir autorización de los titulares para seguir tratando sus datos personales. De no ser ello factible, el tratamiento debe finalizar.

199. En general, la Guía subraya la importancia de ofrecer orientación a quienes instalen y usen sistemas de video vigilancia, de modo que se ajusten a las normas sobre protección de datos personales. De igual forma, indica que su sentido y razón de ser consiste, ciertamente, en precisar aspectos que deben ser atendidos, con el fin de asegurar la protección de los derechos de quienes fungen como titulares de la información, cuyas imágenes resultan captadas por estos sistemas.

200. Trae a colación que tanto los responsables, como los encargados del tratamiento de datos están sujetos a cumplir las obligaciones derivadas de la Ley Estatutaria sobre el Régimen General de Protección de Datos Personales. Además, pone especial énfasis en que los responsables del tratamiento forzosamente deben tener en cuenta que “por el hecho de contratar a un tercero –Encargado- no se pueden sustraer de sus obligaciones, ya que son los primeros llamados a garantizar que el tratamiento de los datos personales se realice con arreglo a los principios establecidos en la ley y respete los derechos de los titulares” . El documento destaca, igualmente, que cuando la grabación tiene lugar en un ámbito exclusivamente personal o doméstico y los datos captados no se encuentran destinados a circular, sino que son preservados en la esfera íntima de la persona natural, entonces no le será aplicable el régimen de protección de datos.

201. De otra parte, menciona que, dados los lugares en los que suelen instalarse los sistemas de videovigilancia –por ejemplo, establecimientos de comercio, edificios, copropiedades, centros comerciales, parqueaderos, entre otros-, resulta imprescindible informar a los titulares de los datos personales que se encuentran en una zona de videovigilancia y obtener

su autorización para el tratamiento de estos datos. Para que se entienda que la persona titular de la información ha dado su aprobación, es necesario que esta la exprese por escrito, verbalmente o mediante conductas inequívocas que no den lugar a dudar o, permitan concluir de modo razonable, que la autorización fue otorgada –se destaca-. En tal caso, el silencio no podría hacerse equivalente a una conducta inequívoca.

202. Entre los aspectos importantes que trae la Guía en comentario, se encuentra también que tanto los responsables como los encargados del tratamiento de datos están obligados a determinar, previamente, los procedimientos vinculados con la actividad de recolectar, mantener, usar, suprimir o disponer de los datos personales y lo relativo a las peticiones, consultas reclamaciones que presenten los titulares, concordantes con el objetivo o propósito del sistema de videovigilancia. Estos procedimientos deben poder ser conocidos por el personal que tendrá acceso a los sistemas.

203. La Guía también contempla la necesidad de que los sistemas de videovigilancia y, la base de datos que surge a partir de su instalación cuente con medidas de orden técnico, humano, administrativo indispensables para afianzar la seguridad de los datos personales y evitar que estos se adulteren, pierdan o deterioren –se destaca-. Estas medidas deben impedir, asimismo, su consulta, uso o acceso no autorizado o fraudulento y proveer porque se mantenga la integridad de la información y se garanticen los derechos de los titulares de los datos personales –se destaca-. Con ese propósito, los responsables y encargados del tratamiento de datos están obligados a adoptar las medidas que estimen efectivas y pertinentes para que la información sea debidamente protegida –se destaca-. La guía trae como ejemplo, las siguientes: “limitar el acceso a la información, cifrar la información y realizar auditorías periódicas a las medidas adoptadas” .

204. Un aspecto especialmente relevante que contiene la Guía tiene que ver con que los “datos personales recolectados deberán mantenerse sólo por el tiempo que sea necesario, de acuerdo con la finalidad específica establecida por el responsable del tratamiento, al cabo del cual deberán ser eliminados” –se destaca-. De igual manera, resalta la importancia de que los procesos de eliminación de la información queden debidamente documentados y

advierte que “las medidas de seguridad implementadas dependerán del análisis de riesgo que se realice en cada etapa del ciclo del dato tratado, es decir, desde el momento en que se recolecta hasta su disposición final” -se destaca-.

205. El documento expedido por la Superintendencia de Industria y Comercio también recuerda que a los titulares de los datos personales les asiste el derecho de: “i) conocer, actualizar, rectificar o suprimir sus datos personales; ii) revocar la autorización del tratamiento; iii) ser informados acerca del tratamiento de los mismos; a presentar quejas por infracciones al Régimen General de Protección de Datos Personales a acceder de forma gratuita a los datos personales que hayan sido objeto de tratamiento, entre otros.

206. Otro aspecto importante que menciona la Guía es que el titular de los datos personales tiene el derecho de solicitar que se supriman sus imágenes “en la medida en que no exista un deber legal o contractual que impida suprimirlos -se destaca-. Ilustra con un ejemplo el caso en que no opera la supresión, esto es, “cuando los datos personales recolectados mediante una grabación constituyan prueba de la presunta comisión de un delito” -se destaca-. Además, agrega que la supresión u otra reclamación adelantada ante los responsables y encargados del tratamiento tiene que llevarse a cabo acorde con el procedimiento previsto en los artículos 15 y 16 de la Ley 1581 de 2012. Finalmente, sostiene que, de cualquier manera, las imágenes no pueden ser retenidas de manera indefinida en el tiempo. Por el contrario, el término de retención “debe ser limitado y razonable” -se destaca-.

c) Importancia de acotar los objetivos o fines que justifican los circuitos cerrados de vigilancia y seguridad para que pueda considerarse una acción legítima en un Estado que se rige por las libertades y derechos de la ciudadanía y que evita instrumentalizar a las personas

207. Como se mencionó, entre los principales motivos para el uso de sistemas de

videovigilancia se encuentra uno común y predominante a nivel mundial: el temor por el delito. Así, con el propósito de proteger personas, propiedades, detectar, prevenir y castigar delitos, entre otros propósitos, se acude a sistemas cerrados de videovigilancia y seguridad privada que captan y graban imágenes y sonidos. Dados sus rasgos característicos, la videovigilancia suele representar una interferencia en el ejercicio de los derechos fundamentales a la intimidad y al hábeas data, pues abre la posibilidad de que seamos observados/as de manera permanente cada vez que transitamos por lugares –públicos o privados–, en los que se acude a esta técnica para vigilar. Como bien señala la doctrina –se mantienen las notas a pie de página en el texto citado; se destaca–:

ser examinados por una cámara, que en muchas ocasiones conserva una copia de la grabación, no es lo mismo que ser contemplados por una persona. En el primer caso, la vigilancia es con carácter general más prolongada, más intensa, más detallada. No permite interrogar a la persona que se encuentra detrás y, en consecuencia, es difícil para nosotros saber cómo responder a ese seguimiento o decidir qué podemos hacer al respecto. Desconocemos qué imágenes obtenidas por las cámaras se conservarán o quién tiene acceso a ellas, tampoco, en consecuencia, podemos tener la certeza de que no sean malinterpretadas o utilizadas de modo inaceptable.

i. i. Riesgos relacionados con la aplicación de sistemas de videovigilancia

208. Ahora bien, es de anotar que, ante una vigilancia continua y generalizada, se suele modificar el comportamiento, hasta el punto de que bien de modo inconsciente o, de manera consciente, se tiende a censurar la propia forma de actuar y de comunicarse, lo que, sin lugar a duda, interfiere negativamente en la esfera más personal e íntima de cada cual. Tal situación muestra, claramente, la delgada línea que se cruza cuando se acude a la referida tecnología, principalmente, en lugares que se califican como privados, pues los circuitos

cerrados de vigilancia y seguridad se encuentran instalados, comúnmente, en el ingreso a edificios de vivienda o espacios en los que únicamente sus habitantes y visitantes gozan del derecho a entrar y salir. También cuando la videovigilancia privada se instala en lugares de acceso público.

209. Por lo general, se admite que la videovigilancia tiene un propósito doble: prevenir el delito y, al mismo tiempo, obtener elementos de convicción suficientes para perseguir e incriminar a quienes delinquen. Es indudable que estas finalidades pueden cumplirse de modo más efectivo cuando las imágenes captadas por las cámaras son “almacenadas”. De todos modos, esto implica, sin duda, una mayor afectación negativa de los derechos fundamentales a la intimidad y al hábeas data, lo que exige que esta tecnología sea instalada de forma que limite lo menos posible los derechos y libertades fundamentales.

210. En efecto, instalar sistemas de circuito cerrado de vigilancia y seguridad privada ha servido para prevenir que se cometan delitos y también para perseguir y encontrar a quienes han delinquido. Es por ello, por lo que en la actualidad el uso de esa tecnología cuenta con una extendida aprobación. Sin embargo, su masiva aplicación a lo largo y ancho del globo terráqueo también ha “supuesto en muchos casos un sacrificio excesivo de no pocos derechos y libertades”, entre ellos, los derechos a la intimidad, al hábeas data y aquellos derechos fundamentales relacionados estrechamente con estos, como la preservación de la propia imagen y el libre desarrollo de la personalidad –se destaca-. Unas breves referencias a la doctrina permiten entender mejor las amenazas que se presentan cuando se aplica la aludida tecnología y la imperiosa necesidad de contrarrestarlas –se destaca-:

Tanto bajo la dictadura del nacionalsocialismo como en la DDR [República Democrática Alemana], el uso de los aparatos de reproducción de sonido e imagen constituía una práctica común. El espionaje y la denuncia eran en los dos puntales en los que se apoyaba el poder. De manera obsesiva los partidos y el Estado propugnaban por mantener el control sobre la población. En el ámbito público se utilizaban para vigilar a enemigos, es decir, a los

periodistas del Este, a los defensores de los derechos, a los manifestantes y a todas las personas, en general, críticas con el régimen. Los sistemas de videocámaras eran odiados y temidos por una gran parte del pueblo alemán. Muchos ciudadanos no confiaban en poder hablar abierta y libremente en sus propias casas porque incluso allí eran espiados. Los más beligerantes con el Gobierno tenían pinchados sus teléfonos lo que suponía un atentado muy grave contra su privacidad. La película *La Vida de los otros* ilustra de forma clara la situación sufrida en aquellos años en la RDA [República Democrática Alemana].

211. Es cierto que los referidos sucesos han sido, en buena hora, superados en Alemania. No obstante, deben ser recordados una y otra vez, para impedir que se repitan. Esta memoria histórica es aún más necesaria cuando se considera que conciliar la seguridad con la protección de derechos y libertades fundamentales no puede calificarse como algo obvio. Enfrentada a la inseguridad del mundo que se vive en la actualidad, la protección de los derechos y libertades fundamentales suele retroceder. Desde ese horizonte de comprensión, la videovigilancia continúa presentando interrogantes inquietantes –se mantienen las notas a pie de página en el texto citado–:

¿Qué se puede filmar? ¿Hay un derecho a la vida privada en el espacio público? y en caso afirmativo ¿cómo proteger este derecho? ¿Es posible evitar la discriminación de algunos grupos y de qué forma se puede poner esta herramienta de vigilancia a disposición de toda la población? ¿Qué hacer para que la videovigilancia funcione y cuando recurrir a otros instrumentos? ¿De qué manera se puede utilizar la videovigilancia con los ciudadanos como herramienta para prevenir la criminalidad y garantizar la tranquilidad pública?

213. En contraste con lo sucedido en Gran Bretaña, en Alemania el uso de la videovigilancia no se inició tan temprano y tampoco se desarrolló de manera acelerada. Esto se debe, en gran parte, a la importancia que para el pueblo alemán tiene la protección de los derechos

fundamentales, luego de padecer duras experiencias en las que estos bienes jurídicos fueron vulnerados de manera absoluta. Estas vivencias amargas han llevado a los alemanes a conferirle una especial atención al tema de la protección de datos y ha permitido observar que la “videovigilancia es el clásico ejemplo del conflicto entre la técnica de la vigilancia y el derecho a la autodeterminación informativa: los afectados no saben, quién y qué se esconde detrás de la cámara de observación” –se destaca–.

. ¿Cómo se han enfrentado los retos en el derecho comparado? Importancia que se le confiere a la aptitud y necesidad de la medida

214. Las ordenaciones de los países europeos son diferentes y uno de sus rasgos característicos es, precisamente, su falta de homogeneidad. Por ese motivo, la regulación europea se ha dirigido, en general, a incentivar la armonización de legislaciones y, en ese sentido, a adoptar normas para garantizar que i) la recopilación efectuada por circuitos de videovigilancia sea lícita y leal; ii) las grabaciones y registros persigan finalidades legítimas; iii) las imágenes sean conservadas por un tiempo estrictamente indispensable iv) el sistema no se use de manera excesiva, así como se mantenga en una relación de proporción respecto de los fines que se busca alcanzar, cerciorándose de la pertinencia de los datos y de que se cumpla con el deber de actualizarlos; v) no se traten datos sensibles relacionados con raza, opiniones políticas, salud, religión, vida sexual; vi) se garantice el derecho de las personas a conocer la información sobre ellas almacenada y a exigir que las rectificaciones sean precisas; vii) se informe con claridad y de manera adecuada a las personas, indicando la finalidad del sistema y, al paso, también la identidad de los responsables; viii) se proteja el derecho de las personas eventualmente afectadas a consultar sus imágenes y grabaciones y ix) se haga efectiva la seguridad e integridad de todos los afectados, acudiendo a toda medida técnica y organizativa necesaria.

215. Una contribución importante del sistema europeo es la figura del Supervisor de Protección de Datos –CEPD–, autoridad independiente que tiene a su cargo tanto asegurar

que las reglas se respeten, como ejercer el control sobre el tratamiento de datos personales efectuado por las instituciones europeas –se destaca–. El 17 de marzo de 2010, este órgano publicó un grupo de lineamientos sobre la videovigilancia con recomendaciones prácticas. Se trata de normas técnicas de precaución “que permiten proteger mejor los datos de carácter personal y la vida privada de las personas filmadas y deben estar incorporadas, desde la etapa inicial de diseño, en las características tecnológicas de los sistemas de vigilancia”.

216. La existencia de esta figura reviste especial importancia, pues entre los desafíos que se presentan se encuentra la necesidad de acotar las finalidades que se buscan con la aplicación de este tipo de tecnología –se destaca–. La dificultad tiene que ver con la amplitud con que se suelen formular las finalidades perseguidas. En el derecho alemán se habló, inicialmente, de “salvaguardar intereses legítimos”. Ante la excesiva falta de precisión de estos términos, se propuso que las finalidades debían ser expuestas de modo más concreto. Sin embargo, esta solución también resultó insuficiente, puesto que no se reguló “el cuándo, el dónde y a quién” le corresponde verificar que se cumplan los objetivos.

217. De ahí que la indeterminación no haya podido ser superada y que cobre una relevancia central la alternativa de contar con una autoridad independiente encargada de examinar si los fines se ajustan a lo previsto en el ordenamiento y de evitar que estos sean cambiados de manera discrecional como, en ocasiones, sucede en la práctica.

218. Si bien en Colombia no existe una autoridad independiente para garantizar que se cumplan rigurosamente las finalidades que se persiguen con la videovigilancia, la Guía para la Protección de Datos Personales en Sistemas de Videovigilancia expedida por la Superintendencia de Industria y Comercio en el 2016, incorpora normas con contenidos similares a las europeas, como quedó visto. Además, el referido documento puso un especial énfasis en la importancia de verificar que esta tecnología resulte, efectivamente, adecuada y necesaria para obtener los propósitos fijados y no exista otra medida que sea menos invasiva e interfiera de menor manera en el ejercicio de los derechos fundamentales a la intimidad y

al hábeas data por parte de las personas eventualmente afectadas.

219. Bajo esa óptica, la aptitud y necesidad de la medida debe examinarse de manera cuidadosa y, con especial rigor, más aún si se considera que la seguridad y la prevención del delito se puede lograr acudiendo a otros medios menos invasivos de los derechos fundamentales a la intimidad y al hábeas data, como, por ejemplo, mejorando los sistemas de iluminación o vinculando personal adecuado para el efecto. Por tanto, cuando quiera que existan alternativas que interfieran en menor forma otros bienes jurídicos en juego, deben preferirse y ha de renunciarse a grabar de manera genérica y amplia. Lo anterior, tanto más si existen motivos que permitan concluir que las personas observadas pueden sufrir un grave menoscabo en sus derechos y libertades fundamentales.

220. A propósito de este tema, la doctrina ha subrayado un aspecto importante relacionado con la calidad de las grabaciones. Así, ha destacado que aquellas que tienen lugar en parqueaderos privados de una vivienda suelen no generar conflicto, en la medida de que cuentan con una baja resolución. Sin embargo, se ha advertido acerca de que los problemas en lugar de disminuir se agravan cuando se toma nota de que los “modernos sistemas de videovigilancia poseen una resolución cada vez mayor, lo que representa una amenaza constante para los derechos de la personalidad”.

221. Ahora bien, es claro que, tratándose de circuitos cerrados de vigilancia y seguridad privada, las expectativas razonables de privacidad deben preservarse, al margen de si los sistemas se encuentran ubicados en el espacio público o en el privado. No obstante, en este último ámbito el interés por una mayor protección de estas expectativas suele aumentar, pues esos espacios albergan de manera más aguda la intimidad de las personas, por lo que cualquier interferencia estatal o de terceros debe ser marginal o menos intensa y someterse a un escrutinio estricto de proporcionalidad.

. La importancia de examinar con detalle la situación concreta y de discernir en cada asunto cómo puede verse afectada la expectativa razonable o legítima de privacidad

222. Respecto de todos estos temas, la doctrina y la jurisprudencia comparadas han hecho grandes aportes. Así, en relación con la necesidad de protección frente a circuitos cerrados de seguridad y vigilancia privada ubicados en lugares públicos han resaltado la importancia de examinar con cuidado la situación concreta –se destaca–. En ese mismo orden, han llamado a distinguir los ámbitos en los que “el desarrollo de la personalidad o la garantía de los derechos de la libertad tienen una gran relevancia, de aquellos en que estos bienes jurídicos revisten una importancia menor. Para solucionar los conflictos que suelen suscitarse, la jurisprudencia acostumbra a discernir, en cada caso, cuál es la expectativa razonable o legítima de privacidad que puede verse afectada.

223. Esto se refleja, por ejemplo, en la decisión adoptada por el Tribunal Supremo (Bundesgerichtshof) alemán, el 8 de abril de 2011, relacionada con la instalación de una cámara de videovigilancia y seguridad en el punto de ingreso de una vivienda. En este caso, la cámara se activaba de manera automática cada vez que se escuchaba un timbre y no se producía ningún almacenamiento posterior de la imagen captada, cuya duración era únicamente de un minuto. El alto Tribunal concluyó que la aplicación de este sistema de videovigilancia se ajustaba a derecho, pues su objetivo era preservar la vivienda del accionado de eventuales injerencias externas (Hausrecht).

224. Para el Tribunal Supremo la medida no solo debía considerarse jurídicamente válida, sino que, en su criterio, no existía una alternativa menos invasiva de los derechos de las personas eventualmente afectadas. Además, el alto Tribunal tampoco encontró que la expectativa de privacidad de las personas posiblemente concernidas tuviera que ser reconocida de manera preponderante, pues, la eventual restricción de este bien jurídico se encontraba temporalmente limitada y se contraía a permitir que el dueño estuviera en condición de establecer quiénes visitaban su vivienda para autorizar o negar su ingreso.

225. En otra decisión muy ilustrativa, el Tribunal Superior de Hamburgo (Alemania), mediante sentencia del 22 de abril de 2008, se pronunció sobre el caso del dueño de una cadena de cafeterías que resolvió instalar en sus locales sistemas de videovigilancia. Estos circuitos fueron ubicados en distintos espacios, incluso, en lugares en los que se captaba a los clientes cuando se sentaban a conversar y a degustar sus consumos. Un cliente frecuente consideró que la instalación de estas cámaras vulneraba su derecho a la autodeterminación informativa.

226. El dueño de las cafeterías alegó como defensa la doble finalidad –preventiva y represiva–, que en su caso tenía la instalación de circuitos de videovigilancia, en tanto intereses legítimos y dignos de protección. El Tribunal admitió que la instalación de la tecnología mencionada era necesaria, pues la presencia de un vigilante como testigo ocular carecía de la efectividad que tienen los circuitos cerrados de vigilancia y seguridad. Sin embargo, dejó claro que en el asunto bajo examen resultaba preciso diferenciar los lugares en los que quedaron instalados los sistemas de videovigilancia. Por un lado, aquellos ubicados en las estanterías y cerca de los puntos de pago y, por el otro, los situados en los lugares en los que se congregaba la clientela para conversar tranquilamente y efectuar sus consumos.

227. La mencionada autoridad judicial indicó que, en estos últimos espacios, la interferencia en el derecho fundamental a la autodeterminación informática era mucho más aguda, siendo que no se correspondían, precisamente, con aquellos en los que suelen producirse robos de dinero o sustracción ilícita de productos. Concluyó que sólo en estos últimos sitios la medida podía considerarse ajustada al ordenamiento, mientras que “en los lugares de reunión en donde los clientes conversan y disfrutan de sus consumos no existe ningún peligro y, por tanto, no tiene sentido la colocación de estos sistemas”. El Tribunal subrayó que por tratarse de espacios en los que la clientela permanece observada de manera prácticamente continua, sus derechos de la personalidad pueden verse gravemente amenazados.

228. El Tribunal Europeo de Derechos Humanos ha protegido, asimismo, la expectativa razonable de privacidad, incluso, en casos en los que los circuitos de vigilancia y seguridad privada se encuentran instalados en el espacio público. Esto sucedió, por ejemplo, con el intento de suicidio de una persona que fue captado por un circuito cerrado de televisión ubicado en el espacio público y cuya videograbación fue entregada, luego, a los medios de comunicación.

229. En aquella oportunidad, el alto Tribunal sostuvo que “la videovigilancia de lugares públicos entra dentro del alcance del artículo 8º de la Convención Europea de Derechos Humanos cuando los datos visuales se graban, se almacenan y se hacen públicos”. Destacó, igualmente, que entregar a los medios de comunicación, para su difusión, un vídeo relativo al intento de suicidio de una persona captado por un circuito cerrado de televisión debía considerarse como una injerencia grave en su vida privada, pese a que el hecho fue captado por un sistema ubicado en un lugar público. De todas maneras, insistió en que si tenemos privacidad (o expectativa de privacidad) en el espacio público, con mayor razón esa expectativa aumenta en cuanto los espacios se hacen semiprivados o privados –se destaca–.

. Los lineamientos derivados de la jurisprudencia proferida por la Corte Constitucional

230. Esta Corporación también se ha pronunciado sobre el tema en varias oportunidades y, más recientemente, en la sentencia T-280 de 2022. En esta providencia efectuó un recuento completo de su jurisprudencia y extrajo, entre otros aspectos, las siguientes conclusiones sobre la instalación de cámaras de videovigilancia y seguridad.

Primero, que instalar sistemas de vigilancia en espacios laborales no desconoce derechos fundamentales a la intimidad, a la dignidad humana, al debido proceso y al trabajo en condiciones dignas y justas, cuando existe una motivo constitucionalmente legítimo o válido que lo justifique.

Segundo, que para determinar si la finalidad es válida y, al paso, es también necesaria y proporcionada, resulta indispensable constatar cuál es el objeto social que cumple la empresa.

Tercero, que se debe considerar el lugar en el que se instalan las cámaras para evitar invadir de manera arbitraria espacios abiertos al público en los que la expectativa razonable de privacidad resulta ostensible, por ejemplo, baños.

Cuarto, que el propósito de la videovigilancia debe relacionarse con una medida de seguridad necesaria, lo que supone examinar si existen formas que invadan en menor proporción los derechos fundamentales de las personas que pueden verse afectadas.

Quinto, que la medida consistente en instalar cámaras de vigilancia por motivos de seguridad sea dada a conocer a las personas eventualmente afectadas.

Sexto, que se excluya todo trato inhumano, cruel o degradante derivado de la medida de seguridad.

Séptimo, que cuando con la instalación de cámaras de vigilancia puedan afectarse los derechos fundamentales de niños, niñas y adolescentes que son sujetos de especial protección constitucional, se debe aplicar un juicio de proporcionalidad estricto.

Octavo, que, si bien instalar cámaras de vigilancia en instituciones educativas tiene un

propósito que puede considerarse constitucionalmente válido, a saber, la seguridad de las y los estudiantes, acudir a esta tecnología no respeta la exigencia de necesidad, toda vez que existen otros mecanismos que cumplen el mismo objetivo y son menos lesivos del derecho fundamental a la intimidad.

Noveno, que instalar sistemas de videovigilancia en instituciones educativas no solo afecta de manera desproporcionada los derechos fundamentales de las y los estudiantes. Inhibe las expresiones y manifestaciones características de estos entornos escolares y constituye una auténtica panoptización.

Décimo, que una entidad de carácter privado no está obligada a entregar copias de los videos de seguridad que captaron imágenes de la vía pública, solicitadas con la finalidad de ser allegadas a un proceso penal, puesto que esta información tiene carácter reservado y solo puede ser entregada en virtud de una orden judicial. En ese sentido, la información obtenida en virtud de grabaciones de video de la calle o el espacio público se cataloga como privada.

Decimoprimer, que “la entrega de material fílmico a los particulares puede vulnerar el derecho a la intimidad de las terceras personas porque su imagen pudo quedar registrada en la grabación solicitada por el ciudadano”.

Decimosegundo, que “el material fílmico se debe reclamar, tratar, cuidar, custodiar y proteger” por las autoridades competentes.

Decimotercero, que, tratándose de un proceso penal, le corresponde a la Fiscalía General de la Nación incorporar la prueba.

Decimocuarto, que “los registros audiovisuales contenidos en las cámaras de seguridad de un establecimiento público que incluyen imágenes privadas de los niños, las niñas y los adolescentes (i.e. imágenes en vestido de baño) constituyen información privada” y solo puede ser obtenida por orden de una autoridad judicial en cumplimiento de sus funciones”.

Decimoquinto, que la medida consistente en instalar cámaras de video vigilancia en medios de transporte público masivo se encuentra justificada porque persigue un objetivo legítimo, a saber, preserva el interés general de la población y cumple además con los requisitos de proporcionalidad y razonabilidad exigidos por la jurisprudencia constitucional.

Decimosexto, las expectativas razonables de privacidad deben preservarse, al margen de si los sistemas se encuentran ubicados en el espacio público o en el privado.

231. La Corte Constitucional también se ha interrogado sobre “la naturaleza de la información [que podría quedar afectada con la instalación de sistemas de videovigilancia] y su mayor o menor vinculación con la intimidad del titular”. En general, ha ofrecido una tipología que clasifica la información en pública, semiprivada, privada y reservada.

232. Al respecto, la Corte ha subrayado que los distintos niveles de protección obedecen a la aplicación de los principios previstos por la Ley 1581 de 2012 Estatutaria sobre la Protección de Datos Personales a la que se hizo mención líneas atrás y, particularmente, al principio de finalidad, según el cual resulta necesario “que el tratamiento de los datos obedezca a una finalidad legítima, de acuerdo con la Constitución y la ley; objetivo que, a su vez, debe ser informado al titular de la información” –se destaca–.

233. En su tarea de establecer el alcance del principio de finalidad, la Corte Constitucional ha descrito sus rasgos característicos, en el sentido de que la actividad de acopiar, procesar y divulgar información personal “debe obedecer a un fin constitucionalmente legítimo”, definido de manera clara, suficiente y previa”. Lo anterior supone, que queda prohibido i) recopilar información personal, sin establecer el motivo por el cual se incorpora en una base de datos, así como ii) recolectar, procesar y divulgar información personal para un propósito diferente al inicialmente previsto y permitido por el titular de los datos, cuando está de por medio una expectativa razonable de privacidad –se destaca–.

234. En general, la jurisprudencia constitucional ha insistido en la necesidad de cumplir con las exigencias derivadas de la regulación constitucional, legal y reglamentaria vigente, así como de ponderar a la luz de las circunstancias del asunto en particular si: i) recoger, tratar o usar datos personales es indispensable para alcanzar los fines previstos; ii) no existen otros medios más apropiados y menos invasivos de los derechos fundamentales a la intimidad y al hábeas data; iii) la medida es necesaria o imprescindible para la finalidad prevista, porque no basta acudir a medios alternativos para lograr idénticos propósitos. Por último, debe insistirse en que, de acuerdo con las normas vigentes, la finalidad debe establecerse, inicialmente, desde el momento en el que se instala el sistema de videovigilancia y seguridad, propósito que no puede ser modificado posteriormente.

. Balance

235. Como puede verse, la regulación europea coincide en algunos puntos con la vigente en Colombia. No obstante, hay elementos de suma relevancia que no están contemplados en la normatividad legal que rige la videovigilancia en el país, así algunas de estas previsiones hayan sido objeto de ordenación mediante reglamento (Guía para la Protección de Datos Personales en Sistemas de Videovigilancia expedida por la Superintendencia de Industria y Comercio en el año 2016).

236. Por ejemplo, las medidas relacionadas con: i) impedir recopilar, indexar, conservar o comparar innecesariamente datos; ii) no autorizar la videovigilancia si el tratamiento de los datos facilita discriminar sectores de la población o grupos de personas por motivo de su opinión política, de sus convicciones religiosas, de su vida sexual, de sus características raciales o étnicas; iii) adoptar disposiciones orientadas a restringir la instalación de equipos de videovigilancia teniendo en consideración el lugar objeto de vigilancia y tomando en cuenta que zonas privadas deben ser excluidas del ámbito de la videovigilancia; iv) valerse de un software apropiado que permita codificar criptográficamente los vídeos, así como crear mecanismos de acción jurídica cuando se presente el uso abusivo de las técnicas de imagen y v) acotar de manera más precisa las finalidades que se busca cumplir con la aplicación de sistemas de videovigilancia, especificando, de manera clara, directa y, precisa, “el cuándo, el dónde y a quién” y comunicar esta decisión a una autoridad efectivamente independiente encargada de verificar que estas finalidades se cumplen con rigor y no se cambian de modo discrecional –se destaca–.

237. Hay otros aspectos que también deberían ser tenidos en cuenta en el momento de ponderar entre los bienes jurídicos en tensión –se destaca–. Pueden mencionarse, de manera indicativa, los siguientes: i) si la observación que se efectúa mediante circuitos cerrados de vigilancia y seguridad privada es permanente o limitada en el tiempo; ii) si las cámaras son fijas o móviles; iii) cuál es la calidad de la resolución de las imágenes captadas; iv) en qué medida es factible eliminar la grabación a la que se ha accedido cuando ya no sea útil; v) si es posible crear protocolos que limiten el número y la calidad de los espectadores de los videos capturados o que especifiquen las imágenes necesarias para cada finalidad y vi) cuál es la expectativa de privacidad considerando el lugar en el que se instala el sistema de videovigilancia y seguridad, incluso, cuando este se ubica en espacios públicos o semipúblicos.

238. De todas formas, es de resaltar que, si los sistemas de videovigilancia se instalan en espacios privados o semiprivados, como edificios o, lugares de habitación, la expectativa de

intimidad es alta o máxima. Esto de ninguna manera significa que en el espacio público o semi público la expectativa razonable de privacidad no deba ser protegida –se destaca-. Para establecer la amplitud con que la expectativa razonable de privacidad debe ser salvaguardada, resulta indispensable analizar, en detalle, las características del caso concreto.

239. Las anteriores consideraciones permiten a la Corte resaltar la importancia de acotar los objetivos o fines que justifican la tecnología de circuitos cerrados de seguridad y vigilancia privada para que pueda considerarse legítima en un Estado que se rige por las libertades y derechos de la ciudadanía y que evita instrumentalizar a las personas. No solo se trata de limitar la finalidad y el uso de la información recopilada, sino de implementar todas las garantías compatibles de los derechos fundamentales a la intimidad y al hábeas data.

d) Criterios fijados por la jurisprudencia constitucional para ponderar el conflicto entre, de un lado, la seguridad y la vigilancia y, del otro, los derechos fundamentales a la intimidad y al hábeas data, cuya vigencia se relaciona –estrechamente-, con la necesidad de respetar la dignidad humana, la libertad y la autonomía de las personas.

240. En efecto, la jurisprudencia constitucional ha reiterado que el derecho fundamental a la intimidad –lo propio sucede con el derecho fundamental al hábeas data-, puede entrar en conflicto con otros derechos fundamentales o con bienes superiores del ordenamiento y, en esa medida, no se trata de derechos que se protejan con carácter absoluto. Sin embargo, ha advertido, igualmente, que debe salvaguardarse su núcleo esencial –se destaca-.

241. Líneas atrás se señaló que el derecho a la intimidad se vincula con distintos aspectos de la existencia, entre estos, aquella dimensión personalísima no susceptible de interferencias constitucionalmente injustificadas por parte del Estado, ni de terceros. Consiste en una esfera en la que la persona se determina autónomamente y se apropia de los elementos que le permiten desarrollar una vida familiar, social, política y cultural plena que se concreta en

“poder actuar libremente en la mencionada esfera o núcleo, en ejercicio de la libertad personal y familiar, sin más limitaciones que los derechos de los demás y el ordenamiento jurídico”. A lo anterior se agrega que, tratándose del ámbito de protección del derecho fundamental al hábeas data, cuestiones asociadas con el ámbito personalísimo de quienes son titulares de ese derecho no pueden ser divulgadas sin su autorización.

242. Con todo, debido a su naturaleza relacional, los derechos fundamentales a la intimidad y al hábeas data tienen también un carácter disponible. Esto se traduce en que, a lo largo de la vida, quienes son sus titulares pueden, con ocasión de las múltiples relaciones interpersonales que se presentan, renunciar a la protección absoluta de estos derechos o ser impelidos a ceder en esa protección cuando así lo exige la prevalencia del orden social y el interés general. En fin, el ejercicio de estos derechos fundamentales puede retroceder, asimismo, ante el surgimiento de conflictos con otros derechos y principios.

243. Si bien la jurisprudencia constitucional ha reiterado que los derechos fundamentales a la intimidad y al hábeas data no son absolutos e, incluso, pueden ser disponibles por sus titulares, ha insistido, asimismo, en que cualquier restricción que se imponga debe fundamentarse en un motivo constitucionalmente válido y respetar el núcleo esencial de estos derechos, lo que supone verificar que la medida a la que acude el poder de intervención estatal o de la sociedad sea razonable y no arbitraria, esto es, que sea válida, apta, necesaria y estrictamente proporcionada -se destaca-.

244. Es importante recalcar nuevamente en este lugar que prevenir, perseguir y sancionar conductas que atentan contra personas y bienes constituye una razón constitucional válida e incluso imperiosa para restringir los derechos fundamentales a la intimidad y al hábeas data -se destaca-. Igualmente, es relevante resaltar que la intromisión estatal o de terceros en derechos fundamentales como los mencionados debe fundarse en motivos clara y precisamente establecidos por la ley, previa autorización judicial -se destaca-. En síntesis, se exige que la medida i) se apoye en un motivo previsto por la ley; ii) determine los lugares en

los que se hará efectiva y, en caso de no poder determinarlos, los describa detalladamente y
iii) evalúe si la medida es proporcional. Como ya quedó expuesto, en casos de flagrancia o, tratándose de medidas urgentes, la intervención judicial puede ser posterior –se destaca–.

10. Examen de constitucionalidad de la disposición acusada

245. Según el demandante, el Legislador incurrió en una omisión legislativa relativa al expedir el artículo 48 de la Ley 2197 de 2022, en cuanto facultó a la Policía Nacional con el objeto de acceder a circuitos cerrados de vigilancia y seguridad privada para acciones de prevención, identificación o judicialización sin restricción alguna y, en esa medida, habría quebrantado los artículos 15 de la Carta Política, 12 de la Declaración Universal de los Derechos Humanos 11 de la Convención Americana sobre Derechos Humanos, 17 del Pacto Internacional de Derechos Civiles y Políticos y 4º, 5º y 6º de la Ley Estatutaria 1581 de 2012 “por la cual se dictan disposiciones generales para la protección de datos personales”.

246. En líneas precedentes, al fijar el sentido y alcance de la disposición acusada, la Sala precisó que esta facultó a la Policía Nacional para efectuar el manejo de datos personales en dos sentidos. En primer lugar, en el acceso a los datos registrados en circuitos cerrados de vigilancia y seguridad privada y, en segundo lugar, con el propósito de usar la información allí registrada para acciones de prevención, identificación o judicialización. En los dos supuestos la potestad conferida a la mencionada autoridad es absoluta, esto es, no se encuentra sujeta a condición o requerimiento alguno.

247. Antes de responder al interrogante planteado por el demandante, a propósito de la alegada omisión legislativa relativa, la Sala contestará la pregunta acerca de si, ¿a la luz del análisis realizado en precedencia, la autorización que le confiere la norma acusada a la Policía Nacional para acceder a circuitos cerrados de seguridad y vigilancia privada para acciones de prevención, identificación y judicialización resulta estrictamente proporcionada?

-se destaca-.

248. De acuerdo con las consideraciones efectuadas en la presente providencia, la respuesta a este interrogante debe tener en cuenta varios aspectos. Como se expuso, los circuitos cerrados de seguridad y vigilancia privada pueden definirse como “un conjunto de componentes directamente entrelazados, [integrado por] una o varias cámaras de vigilancia conectadas a uno o más monitores o televisores, los cuales reproducen imágenes capturadas que crean un circuito de imágenes”.

249. Estas imágenes pueden quedar almacenadas en medios analógicos o digitales según lo requiera el usuario. Los circuitos cerrados a los que se refiere la norma son aquellos agenciados por empresas de seguridad y vigilancia privada, pero los responsables del manejo de datos son las personas naturales o jurídicas que contratan esos servicios. En ambos casos, estas personas deben cumplir con las exigencias del régimen constitucional y legislativo de protección de datos (Ley Estatutaria 1581 de 2012), así como observar la Guía emitida por la Superintendencia de Industria y Comercio que fueron presentadas de modo detallado líneas atrás.

250. En precedencia se señaló, igualmente, que las empresas de seguridad y vigilancia privada se rigen por el Decreto ley 356 de 1994 y se encuentran supervisadas por la Superintendencia de Vigilancia y Seguridad Privada. Por ese motivo, lo lógico es que, en la medida en que estas empresas de seguridad y vigilancia privada se adecuen a las exigencias constitucionales, legales y reglamentarias, tanto estas como los responsables de los datos -personas naturales o jurídicas que también deben sujetarse con rigor al ordenamiento jurídico que rige la materia-, pueden ejercer sus actividades sin interferencias estatales, salvo que exista un motivo constitucionalmente válido.

251. En las consideraciones de la presente sentencia quedó dicho, igualmente, que la Policía

Nacional debe ejercer las funciones atribuidas por el ordenamiento de acuerdo con los principios de i) legalidad y respeto por los derechos fundamentales y las libertades públicas; ii) necesidad en el sentido de que para preservar el orden público únicamente puede tomar medidas imprescindibles y eficaces y iii) proporcionalidad y razonabilidad, esto es, teniendo en cuenta las circunstancias y fines que se propone alcanzar sin incurrir en actuaciones desmesuradas ni arbitrarias; iv) igualdad es decir sin incurrir en actuaciones injustificadamente discriminatorias.

252. En consecuencia, si la Policía Nacional obra tomando en consideración los principios mencionados, el acceso a circuitos cerrados de seguridad y vigilancia para acciones de “prevención, “identificación” o “judicialización” no tendría, en principio, reparos de constitucionalidad. No obstante, a propósito del asunto que examina la Sala en la presente ocasión es importante anotar varios aspectos.

253. En primer lugar, el carácter irrestricto –se destaca– de la habilitación a la Policía Nacional tanto para acceder a circuitos cerrados de vigilancia y seguridad privada, como para hacer uso de los datos allí registrados. En segundo término, la diferencia de propósitos en relación con los cuales el Legislador facultó a la Policía Nacional con el objeto de hacer uso ilimitado de esos datos: de una parte, para acciones de prevención y, de otra, para acciones de identificación o de judicialización.

254. La Sala encuentra que la intensidad con que se afectan los derechos fundamentales a la intimidad y al hábeas data no es igual tratándose de estas tres modalidades de acción y considera que las debe analizar separadamente. Así las cosas, primero aplicará el juicio estricto de proporcionalidad en relación con la facultad que le otorga la disposición acusada a la Policía Nacional para acciones de prevención y, luego, examinará la proporcionalidad de la habilitación que se le concede a esta autoridad para acciones de identificación y judicialización –se destaca–.

a. a) ¿La facultad otorgada a la Policía Nacional por la norma acusada para acceder a circuitos cerrados de vigilancia y seguridad privada con el propósito de que adelante acciones de “prevención” es estrictamente proporcionada?

255. Como quedó dicho en las consideraciones de la presente sentencia, esta Corte ha reiterado en sus pronunciamientos que, en aquellos casos en los que una medida legislativa suponga maximizar un principio constitucional –vb.gr., la seguridad y vigilancia de bienes y personas–, en desmedro de la protección de derechos fundamentales, tales como el de intimidad y el hábeas data u otros estrechamente relacionados con estos –cuyo núcleo esencial puede quedar sensiblemente comprometido–, se hace indispensable que el juez constitucional acuda a la herramienta hermenéutica de la ponderación.

256. De este modo, tratándose de acciones que puedan afectar la intimidad de las personas y sus datos sensibles directamente asociados a la posibilidad de llevar una vida digna, la Corte debe verificar si la medida expedida por el Legislador, además de fundarse en una finalidad constitucionalmente válida, cumple con las exigencias propias de un juicio estricto de proporcionalidad –se destaca–.

257. Se conoce que el juicio estricto de proporcionalidad está dirigido a establecer si el fin perseguido por la medida contemplada en la norma objeto de acusación no solo es válido sino imperioso. Este escrutinio indaga también acerca de si el medio escogido, además de ser efectivamente conducente, es necesario, esto es, si no puede ser reemplazado por otros menos lesivos para los derechos fundamentales intervenidos. Por último, examina si los beneficios de adoptar la medida exceden o no las restricciones impuestas sobre estos derechos fundamentales; es decir, si la medida es proporcional en sentido estricto –se destaca–.

258. Del análisis efectuado en precedencia se sigue que la medida contemplada en la norma

demandada que autoriza a la Policía Nacional para que acceda a circuitos cerrados de vigilancia y seguridad privada, con el propósito de que adelante acciones de “prevención” busca un fin que puede calificarse como constitucionalmente válido, pues se conecta con la posibilidad de luchar contra la delincuencia que afecta a las personas y a los bienes.

259. En efecto, ante el objetivo constitucionalmente válido e, incluso, imperioso de evitar el delito y proteger a bienes y a personas, las acciones de “prevención” atribuidas por el Legislador a la Policía Nacional podrían encontrarse constitucionalmente justificadas. Sin embargo, un análisis más detenido de lo que está en juego con la tecnología vinculada a los circuitos cerrados de vigilancia y seguridad privada, advierte sobre los riesgos que se asumen en detrimento de la protección de los derechos fundamentales a la intimidad y al hábeas data puestos al otro lado de la balanza.

260. Entre otros aspectos, por la dificultad que, en el caso concreto de las acciones de prevención, se presenta a la hora de aplicar las normas que regulan el manejo de datos y también el reglamento dirigido a garantizar que el uso de la tecnología aplicada se mantenga dentro de los cauces constitucionales, legales y reglamentarios –se destaca–.

261. Como lo trajo a colación la Guía para la Protección de Datos Personales en Sistemas de Videovigilancia expedida por la Superintendencia de Industria y Comercio –a la que se hizo mención, extensamente, en párrafos anteriores–, los sistemas de circuito cerrado de vigilancia y seguridad privada no solo observan o supervisan, sino que también están en condición de recopilar imágenes de personas y, en ese sentido, permite[n] monitorear las actividades de las personas “en escenarios domésticos, empresariales, laborales y públicos” –se destaca–.

262. Es más, el documento referido reconoció que la tecnología de circuitos cerrados de vigilancia y seguridad privada involucra elementos intrusivos de la privacidad como lo son el

monitoreo y la observación de las actividades realizadas por las personas cotidianamente –se destaca-. Tanto así que la propia Guía advierte sobre la importancia de tomar nota acerca de cuan necesario resulta acudir a este instrumento y si este, en efecto, logra cumplir con el propósito esperado o existen herramientas alternativas que puedan aplicarse con un menor impacto en la privacidad de las personas –se destaca-.

263. Con el objeto de ilustrar de manera más clara lo que se encuentra en juego, es importante ahondar un poco más en el análisis de la tecnología que aplican los circuitos cerrados de videovigilancia privada, respecto de la cual se podría afirmar que durante las décadas pasadas transformó de manera radical el propio concepto de intimidad personal y de privacidad, así como el manejo de datos.

264. Lo anterior, hasta el punto en que –como se intentará mostrar en lo que sigue-, resulta, incluso, factible afirmar que la regulación consignada en la Ley Estatutaria 1581 de 2012 y en la Guía proferida por la Superintendencia de Industria y Comercio podría quedar vaciada de contenido cuando se toma en cuenta el avance vertiginoso del fenómeno de la videovigilancia, sin que al mismo tiempo pueda afirmarse, con total certeza, que las autoridades –en este caso la Policía Nacional-, estén en condición de mantener eventuales “acciones de prevención” dentro de las fronteras que marcan la Constitución, la legislación y el reglamento –se destaca-.

265. En efecto, resulta factible afirmar que tratándose de circuitos cerrados de seguridad y vigilancia privada estamos frente a una herramienta de la que se valen las personas para protegerse de la delincuencia y que su uso suele ser hasta cierto punto “consentido”. También es posible sostener que esta práctica se encuentra sujeta a la regulación constitucional, legal y reglamentaria. No obstante, ante la vaguedad, imprecisión e indeterminación de la expresión “para acciones de prevención” que denota el propósito en busca del cual el Legislador facultó a la Policía Nacional para acceder–sin ningún condicionamiento que acote esta facultad-, puede sostenerse, de entrada, que esta

atribución no cumple con ninguna de las exigencias derivadas del ordenamiento jurídico relacionada con el uso de esa tecnología, como se verá a continuación –se destaca–.

266. Arriba se explicó, que la normatividad vigente y la jurisprudencia constitucional han enfatizado la importancia de distinguir entre los derechos fundamentales a la intimidad y al hábeas data. En ese sentido, se ha sostenido que el derecho a la intimidad busca asegurar que las personas cuenten con un ámbito de privacidad en su vida personal y familiar, sin interferencias del Estado, ni de terceras personas. Esto implica que los asuntos concernientes al ámbito personalísimo de cada uno no pueden ser divulgados sin que medie previa autorización –se destaca–.

267. Así, el grado en el que estos circuitos cerrados de vigilancia y seguridad eventualmente interfieren el ejercicio de derechos fundamentales como la intimidad personal y familiar, tanto como el hábeas data exige que cuando se han instalado estos sistemas por entidades privadas –sea por motivos de seguridad o persecución de actividades delictivas– se den a conocer las razones, se ofrezca información al respecto y, al paso, se indiquen las actividades que efectuará el responsable del tratamiento de datos, acorde con la normatividad vigente.

268. Como se indicó en precedencia, esclarecer las finalidades de la vigilancia reviste una importancia crucial, en la medida en que las imágenes captadas y los datos personales obtenidos solo pueden usarse para los objetivos previamente especificados y no para otras finalidades –se destaca–. Además, estos objetivos deben estar relacionados con un interés constitucionalmente legítimo –se destaca–. En cuanto al consentimiento de la persona o personas eventualmente afectadas, resulta importante que sea exteriorizado de manera inequívoca y se funde en un conocimiento informado y específico.

269. Puesto de otra manera: de conformidad con las normas vigentes, es claro que las empresas de vigilancia y seguridad privada deben observar unas exigencias para prestar

este servicio. Por eso es de esperar que estas empresas, en cumplimiento de las normas previstas en la Ley 1581 de 2012 y de aquellas incorporadas en la Guía expedida por la Superintendencia de Industria y Comercio exijan a los usuarios su consentimiento informado para el manejo de datos y que operen de conformidad con el principio de finalidad, así como de acuerdo con los demás principios a los que se hizo mención en las consideraciones de la presente sentencia –se destaca–.

270. Sin embargo, examinada la facultad atribuida en la norma acusada a la Policía Nacional “para acciones de prevención” quedan pendientes varios desafíos, principalmente, que la norma no incluye nada que haga pensar que todas las exigencias previstas en la regulación constitucional, legal y reglamentaria vigente puedan cumplirse, dada la manera ambigua e indeterminada en que la autoridad concernida está llamada a realizar las acciones de prevención –se destaca–.

271. ¿Qué significa prevenir? ¿Cómo puede un titular de datos personales y del derecho a preservar su propia imagen y/o a resguardar su domicilio exigir que se cumpla con el requisito del consentimiento previo, libre e informado o con el principio de finalidad de que trata el artículo 4º de la Ley Estatutaria 1581 de 2012, cuando el mismo hecho de preguntar podría dar al traste con la propia idea de “prevenir”?

272. Al ejercer el control de constitucionalidad del artículo 4º de la Ley Estatutaria 1581 de 2012, la Corte recordó cómo, en virtud del desarrollo tecnológico, la relación de las personas con su entorno se ha redimensionado. Sobre este extremo, destacó que recolectar y almacenar la información era un asunto que inicialmente se encontraba relegado a la esfera íntima de cada ser humano o era conocido, únicamente, por sus más allegados. Sin embargo, advirtió, que esa situación se ha transformado diametralmente “en su entorno y estructura”. Así, en la actualidad los datos personales “se han convertido en una práctica habitual de control y almacenamiento por parte de los sectores tanto públicos como privados”, lo que ha implicado el reconocimiento de nuevos derechos con particularidades propias que “intentan

dar respuesta a las nuevas necesidades históricas, mientras que en otras supone la redefinición de viejos derechos”.

273. La Corte hizo hincapié en que, si es cierto que el tratamiento de datos resulta necesario para asegurar el desarrollo de diversos ámbitos de la vida social, también lo es que puede “lesionar derechos fundamentales”. De ahí que la jurisprudencia y los tratados internacionales sobre derechos humanos hayan establecido un conjunto de principios para la administración de datos personales que deben ser aplicados al momento de ponderar derechos y bienes jurídicos en tensión y, de esta forma, evitar el ejercicio “abusivo y arbitrario de la libertad informática”.

274. El interrogante que surge a continuación es si, en vista de la forma como se maneja la información por medio de la tecnología de circuitos cerrados de vigilancia y seguridad privada resulta, en efecto, factible aplicar los principios aludidos y mantener “las acciones de prevención” dentro de las fronteras constitucionales, legales y reglamentarias el manejo de ese material –se destaca–. La Sala encuentra que, para responder esta cuestión de modo directo, preciso y claro, primero debe considerarse, de manera muy general, la forma como se captura y se guarda un video y, en particular, debe pensarse en lo delicado que resulta el manejo de ese material.

275. Entre los aspectos que vale la pena tener en cuenta, puede mencionarse que el material digital resulta fácilmente manipulable. Esto empieza a un nivel muy básico y tiene que ver con la edición. Por tanto, si se piensa en las acciones de prevención atribuidas a la Policía Nacional por la disposición demandada, cabe preguntarse si ¿resulta preciso acceder al video en toda su extensión, desde que se empezó a grabar hasta que finalizó la grabación? ¿O se necesita un fragmento? De acuerdo con ello, ¿quién determina dónde debe iniciar y dónde finalizar el fragmento? Lo que va antes y lo que va después tiene una importancia central, pues es el contexto el que permite aproximarse a una interpretación del material. Una posible fragmentación resulta, en criterio de la Sala, profundamente riesgosa, pues sin el

conocimiento del contexto, es muy fácil manipular o ser manipulado.

277. Lo expuesto facilita comprender que cuando la disposición demandada faculta a la Policía Nacional con el objeto de que acceda a los archivos de video en los que están contenidos los datos de personas determinadas o indeterminadas “para acciones de prevención”, la información de los circuitos cerrados de seguridad y vigilancia no solo está dando acceso a imágenes –se destaca-. También faculta a esta autoridad para que se aproxime a otra información que es profundamente sensible –se destaca-.

278. Por tanto, tratándose de una acción indefinida, vaga, imprecisa e indeterminada como la de “prevención” para la ejecución de la cual la disposición acusada facultó a la Policía Nacional en la norma acusada, ¿qué significa que la Policía Nacional acceda a circuitos cerrados de seguridad y vigilancia privados para esta clase de acciones?

279. La falta de respuesta directa, clara y precisa del Legislador al interrogante formulado preocupa aún más si se tienen en cuenta los riesgos o problemas asociados con el uso de esta tecnología. Un primer aspecto para tener en cuenta es que en el pasado la información capturada en estos circuitos de vigilancia y seguridad privada podía quedar consignada en cintas magnéticas. Esto significa que el material videográfico tenía un soporte material, un objeto en el que estaba, por así decirlo, “contenido”. En tal virtud, era necesaria la existencia de archivos y de custodios. Para poder conocer el video resultaba indispensable estar en posesión del carrete, la cinta, el casete, etc.

280. En la actualidad esto reviste mayor complejidad. ¿Dónde está, físicamente, la información digital? Cuando se afirma que tal información está “en el computador” suele ser una manera coloquial de hablar del asunto. Sería acaso más correcto decir que está “en la

nube”, pero la descripción también resulta a toda luz vaga. La realidad es que esa información digital sí está consignada en diferentes soportes físicos. Por ejemplo, una parte de ella se encuentra en servidores que las más de las veces no se encuentran en territorio nacional –se destaca–.

281. ¿Quién tiene dominio de esta información? ¿Quién es su custodio? A estos interrogantes de difícil resolución se añaden otros, igualmente, espinosos: ¿acceso a qué, concretamente, tiene en este caso la Policía Nacional para acciones de prevención? Una respuesta fácil, mas no satisfactoria es: a circuitos cerrados de vigilancia y seguridad privada. ¿Qué se quiere decir con esto? ¿A dónde, concretamente, es que se le permite el acceso a la Policía Nacional? ¿A las cámaras de videovigilancia manejadas por las empresas de seguridad y vigilancia privada? O, más bien, ¿a una empresa de software que presta el servicio?

282. Lo que sí se puede dimensionar, si se toma en consideración la cantidad de cámaras que suelen ubicarse en espacios privados con el propósito de que vigilen y provean seguridad, es el raudal de información a la que podría tener acceso la Policía Nacional para adelantar acciones tan vagas e imprecisas como las de “prevención” –se destaca–.

283. Nótese que acá no se está hablando, únicamente, de horas y horas de video, sino de todos los “metadatos” que están vinculados a esas imágenes. Entonces, otorgarle esa potestad a la Policía Nacional para fines de “prevención” significa darle una herramienta que la convierte en un ente de vigilancia y control “panóptico”, como lo señalaron algunos de los intervinientes. Con el fin de entender mejor este riesgo, la Sala encuentra que es importante insistir en la necesidad de comprender el contexto en el que se insertan las cámaras de video y sus “metadatos” y observar que estos interfieren de manera profunda en el ejercicio de los derechos fundamentales a la intimidad y al hábeas data.

284. Hasta hace relativamente poco se consideraba que un video o una fotografía era algo

que simplemente se “veía”, se “observaba”, y que, en consecuencia, era necesario un individuo o grupo de personas para su interpretación, análisis y uso. Sin embargo, hoy el mundo de la información y la tecnología están enmarcados por conceptos como inteligencia artificial, big data, machine learning y algoritmos. Por big data se entiende una inmensa cantidad de datos, estructurados y no estructurados, que ofrecen información de todo tipo. Por ejemplo, en el contexto comercial, estos datos pueden dar información sobre los hábitos de compra que tiene una persona lo que, a su vez, puede servir para saber qué tipo de publicidad se le debe enviar a sus redes sociales. El análisis del big data permite identificar problemas, tendencias y patrones.

285. Como la cantidad de información es tan voluminosa, es muy difícil que un humano ejecute esta tarea. Aquí es donde entra el denominado machine learning. Esta es una rama de la inteligencia artificial que, valiéndose de programas y software especializado, puede analizar toda esa información para identificar patrones y realizar predicciones. Esto permite que los computadores realicen este proceso de manera autónoma. Por supuesto, la Sala reconoce que estas nociones son más técnicas, pero lo dicho revela dos realidades: hay una gran cantidad de información sobre las personas obtenida en espacios en donde se instalan circuitos cerrados de vigilancia y seguridad y existe la tecnología para analizar todos esos datos.

286. En lo que se refiere a la autonomía en relación con el manejo de esta información, vale la pena añadir que, si bien la ejecución es autónoma, los computadores y los programas son el resultado de las intenciones de sujetos específicos. Esto implica que muchas veces replican los estereotipos, prejuicios e intereses de quienes los programan, los fabrican y los usan.

287. A esta altura la Sala considera que es necesario hacer énfasis en algo que tiene que ver directamente con las consecuencias que se desprenden de la disposición demandada. Se conoce que en la actualidad se presenta un gran desarrollo en tecnologías vinculadas al

reconocimiento facial. Ya se mencionó que este tipo de herramientas no necesitan supervisión humana, sino que puede ser realizado por los computadores de manera autónoma. En esa medida, el impacto sobre los derechos a la intimidad, a la dignidad, a la preservación de la propia imagen, al libre desarrollo de la personalidad son profundos.

288. Si además de lo expuesto se tiene en cuenta el desarrollo que hay en inteligencia artificial, puede anticiparse el riesgo que implica que la norma acusada otorgue a la Policía Nacional la facultad de acceder a circuitos cerrados de vigilancia y seguridad privados “para acciones de prevención”. No hay que olvidar que esta autoridad podría acceder, potencialmente, no solo al video, sino a todos los datos asociados con éste (hora, lugar, etc.). Con los medios económicos y tecnológicos adecuados, se estaría habilitando a la mencionada autoridad para ejercer facultades para las que, incluso, podría no estar conceptual, técnica y jurídicamente preparada.

289. Ahora bien, hasta el momento la Sala ha concentrado su atención en las posibilidades y los riesgos generales que tienen las nuevas tecnologías y la complejidad del panorama. Con esto busca marcar énfasis en que el Legislador al redactar la norma acusada hizo caso omiso de los avances tecnológicos y dejó de ver los riesgos a los que exponía a la ciudadanía al concederle a la Policía Nacional la facultad de acceder a los datos registrados en videocámaras de vigilancia y seguridad privada para acciones de “prevención”.

290. Aunado a lo anterior, es necesario ver las implicaciones que eso tiene para los derechos fundamentales a la intimidad personal y familiar, así como al hábeas data de quienes pueden salir afectados con la amplitud y la indeterminación de la facultad otorgada por la disposición acusada a la Policía Nacional, con el propósito de que adelante acciones de “prevención”.

291. Para empezar, cuando se tiene en cuenta la cantidad de información que está almacenada en el material videográfico que se produce día a día, se reconoce que es

prácticamente imposible evitar que las costumbres y rutinas de las personas captadas por esos circuitos cerrados de vigilancia y seguridad privada queden registradas en alguna parte.

292. En este sentido, las videocámaras ubicadas en espacios eminentemente privados como ascensores de conjuntos residenciales, parqueaderos privados, ingreso y salida de unidades residenciales hacen posible rastrear sus actividades cotidianas. No solo eso, sino que permiten, en general, encontrar los patrones que marcan esas rutinas y realizar predicciones. Como se dijo, ni siquiera se hace necesario que esto sea llevado a cabo por una persona en particular, sino que basta tener el acceso a la información (vídeo y metadatos), basta un buen software de reconocimiento facial y la tecnología de inteligencia artificial capaz de analizar esos datos.

293. A lo anterior se agrega que la instalación de circuitos cerrados de seguridad y vigilancia privada convertida, hoy por hoy, en tendencia mundial, no cuenta con la aprobación de todas las personas cuyos movimientos quedan registrados en los videos. Tampoco es claro que pueda darse estricta aplicación a los principios y regulaciones que rigen la aplicación de esta tecnología, que quedaron reseñados en las consideraciones de esta decisión, con lo cual se afectan negativamente o se vulneran de plano los derechos fundamentales a la intimidad y al hábeas data.

294. Retomando lo dicho en las consideraciones de la presente sentencia que coincide también con lo expresado por algunos de los intervinientes: “[e]l derecho a la intimidad siempre mantiene una esfera de protección por su naturaleza ontológica”. Esto significa que, pese a que la expectativa razonable o legítima de privacidad puede variar e incluso las personas pueden –en aras de disuadir a la delincuencia y de proteger a personas y a bienes–, consentir en la instalación de videocámaras de vigilancia y seguridad en lugares privados, la ordenación constitucional de los derechos fundamentales a la intimidad y al hábeas data, así como la regulación legal y reglamentaria que la desarrolla muestra que, incluso en espacios públicos, pero, con mayor razón, en espacios privados “se debe mantener un grado de

garantía de la privacidad”. Esta exigencia se haría imposible de llevar a cabo en un escenario como el que plantea la disposición demandada en punto a la potestad conferida a la Policía Nacional “para acciones de prevención”.

295. En fin, una cosa es que los sistemas de seguridad y videovigilancia privados tengan efectos disuasorios. Otra muy distinta es que se usen para fines de “prevención” –se destaca–. En este último evento el consentimiento de la persona afectada o el conocimiento previo de las finalidades para las cuales se realiza la intervención darían al traste con el propósito de “prevención” que se busca obtener, así que el consentimiento previo, expreso e informado quedaría vaciado de contenido, lo mismo que la aplicación del principio de finalidad y de otros principios previstos en el ordenamiento jurídico que quedaron detalladamente explicitados.

296. En otras palabras: permitirle a la Policía Nacional que acceda al material de video consignado en circuitos cerrados de vigilancia y seguridad privados, para acciones de “prevención” facilita que los dueños de la información sensible registrada en esos circuitos queden expuestos a una intromisión sin límites, contraria a las exigencias previstas en el ordenamiento. La consecuencia directa, como también lo señalan varios de los intervinientes, consiste claramente en inhibirla en relación con “aspectos propios de su personalidad y su vida privada personal y familiar”.

297. Es de insistir en que esta tecnología no se limita únicamente a registrar o captar imágenes, sino que se relaciona estrechamente con los denominados “metadatos”, lo que podría llevar más temprano que tarde a una panoptización de la sociedad, contraria a la protección que ordena ofrecer nuestro ordenamiento constitucional, legal y reglamentario a los derechos fundamentales a la intimidad y al hábeas data.

298. En suma, la Corte considera que, dada la tecnología propia de los circuitos cerrados de vigilancia y seguridad privada, la Policía Nacional no está en condición de ejercer la facultad

atribuida por la norma demandada “para acciones de prevención” de acuerdo con las regulaciones constitucionales, legales y reglamentarias. El carácter vago, impreciso y absolutamente indeterminado de la medida impide contar con criterios claros, precisos y objetivos indispensables para que “las acciones de prevención” puedan considerarse legítimas en un Estado que se rige por las libertades y derechos de la ciudadanía y que evita instrumentalizar a las personas.

299. Aun cuando lo dicho hasta este lugar resultaría suficiente para declarar inexecutable la facultad que el artículo 48 le atribuye a la Policía Nacional con el fin de que acceda a circuitos cerrados de vigilancia y seguridad privada “para acciones de prevención”, la Sala proseguirá con los demás pasos del juicio estricto de proporcionalidad y analizará la idoneidad y la necesidad de la medida –se destaca–.

300. Antes de abordar este análisis, resulta oportuno traer nuevamente a colación distintos pronunciamientos de esta Corporación en relación con la instalación de cámaras de vigilancia y restricciones del derecho a la intimidad en la jurisprudencia de la Corte Constitucional. Como lo señaló la sentencia C-094 de 2020 y, quedó expuesto en otra parte de esta sentencia, la Corte ha analizado si es posible “instalar cámaras de video en lugares de trabajo, establecimientos comerciales y centros educativos y su posible injerencia con el derecho a la intimidad y otros derechos”.

301. En la sentencia C-094 de 2020, esta Corte admitió que su jurisprudencia no ha fijado una metodología única, pues en algunos casos se ha valido de un juicio de proporcionalidad y, en otros, ha estudiado el influjo de distintas “variables a fin de identificar si la medida cuestionada armoniza adecuadamente los propósitos perseguidos por la instalación y el derecho a la intimidad”.

302. Así, por ejemplo, en la sentencia T-768 de 2008, la Sala de Revisión puntualizó que con

el objeto de indagar si instalar cámaras de vigilancia en lugares de trabajo desconocía el derecho a la intimidad, debía apreciarse –se destaca–:

(i) el objeto social que desarrolla la empresa, pues es lógico que las medidas se refuercen en bancos o establecimientos públicos; (ii) el lugar en el que la medida es implementada, pues es razonable que recaiga en lugares donde se desarrolle la actividad laboral que, por ejemplo, se encuentren abiertos al público, pero no lo sería en baños o vestuarios; (iii) la finalidad de la medida, la cual debe guardar una relación directa con la seguridad necesaria de las instalaciones de trabajo o el control del cumplimiento de los deberes y funciones de los trabajadores; (iv) la existencia o no de otras medidas menos invasivas para lograr los propósitos perseguidos; (v) la importancia de reducir los perjuicios derivados de la medida; (vi) el conocimiento de la instalación de la cámara, pues solo de manera excepcional pueden legitimarse medidas subrepticias; y (vii) la prohibición de que la medida someta a la persona a tratos crueles, inhumanos o degradantes.

303. En la sentencia T-407 de 2012, la Sala de Revisión indicó que era imprescindible efectuar un balance entre el derecho fundamental a la intimidad y al libre desarrollo de la personalidad del estudiantado, por una parte y, por otra, el objetivo que se buscaba al instalar con cámaras de vigilancia, esto es, prevenir y mitigar conductas que al interior de los colegios afectan la seguridad e integridad de quienes participan en el proceso pedagógico.

304. Con ese propósito, la Corte efectuó un juicio estricto de proporcionalidad –se destaca– y advirtió que instalar sistemas de video vigilancia dirigidos a lograr la seguridad de estudiantes y de la institución educativa era una medida válida desde el punto de vista constitucional y también era idónea, pues permitía disuadir a los estudiantes de cometer infracciones contra la ley y el reglamento, al paso, que hacía factible identificar a quienes incurren en esas conductas.

305. No obstante, subrayó que esa medida no era estrictamente necesaria, toda vez que había mecanismos alternativos, tales como vincular celadores o implementar programas educativos que resultarían menos lesivos. Añadió “que la medida afectaba desproporcionadamente los derechos de los estudiantes, constituía una auténtica ‘panoptización’ y, por esa vía, inhibía expresiones y manifestaciones propias de entornos escolares”.

306. En las sentencias T-487 de 2017 y T-114 de 2018 las Salas de Revisión de la Corte Constitucional tuvieron oportunidad de pronunciarse acerca de la instalación de cámaras de vigilancia en establecimientos de comercio. En el primer caso, la Corporación concedió la tutela del derecho de petición del accionante, por cuanto la sociedad accionada:

(i) no cumplió con la obligación de suministrar la información o la documentación solicitada; y
(ii) por esa vía vulneró el derecho de acceso a la justicia del accionante, en la medida en que, la solicitud de entrega del documento tenía la finalidad exclusiva de ser aportada a un proceso penal. No obstante lo anterior, no ordenó la entrega de la información al accionante y, en su lugar, dispuso remitirla a la autoridad judicial indicando ‘que la entrega del material fílmico a los particulares, podría comprometer los derechos a la imagen y la intimidad de terceras personas, cuyas figuras, aspecto o apariencia, hayan quedado registradas durante el lapso en el que se realizaron las filmaciones que el peticionario reclama, tratamiento, cuidado, custodia y protección que debe quedar en manos de una autoridad pública (en este caso, del Fiscal del caso), y no de los particulares’.

307. En la sentencia T-114 de 2018, la Sala de Revisión se centró en la naturaleza de la información captada por los circuitos cerrados de televisión y al respecto sostuvo que era relevante tomar nota del lugar en el que se encuentran instaladas las cámaras de vigilancia, vale decir, si se hallan en: i) lugares privados, por ejemplo, en una residencia; ii) establecimientos privados abiertos al público; o iii) establecimientos y/o instituciones públicas.

308. Advirtió que en el asunto examinado los registros audiovisuales captados por las cámaras de seguridad del establecimiento accionado debían catalogarse como información privada, por cuanto versaban sobre información personal de niños, niñas y adolescentes que solo podía ser obtenida por orden de autoridad judicial en el cumplimiento de sus funciones. Concluyó que no existía vulneración alguna al derecho invocado por el accionante, pues la información solicitada no era de carácter público, sino privado y ella solo podía ser obtenida a través de orden judicial.

309. Como quedó expuesto en las consideraciones de la presente sentencia, tanto la doctrina como la jurisprudencia comparada e, igualmente, la proferida por esta Corporación, se han pronunciado sobre los alcances del poder informático.

310. Desde muy temprano esta Corte advirtió que “[e]n las sociedades tecnológicas contemporáneas el manejo sistemático de datos personales sirve a propósitos tan variados como apoyar los procesos de distribución de las cargas y los bienes públicos; facilitar la gestión de las autoridades militares y de policía; o, fomentar el funcionamiento del mercado. En tales condiciones, quien tiene la posibilidad de acopiar, ordenar, utilizar y difundir datos personales adquiere un poder de facto, denominado ‘poder informático’”. Igualmente, ha puntualizado esta Corte que “el abuso o la negligencia en el ejercicio de este enorme poder, apareja un serio riesgo, entre otros, para los derechos fundamentales a la personalidad, a la identidad, a la igualdad, a la intimidad, a la honra, al buen nombre o al debido proceso del sujeto concernido”.

312. Varias de las investigaciones realizadas sobre este tema han encontrado poca correlación entre la cantidad de circuitos cerrados de vigilancia y seguridad y el crimen o la seguridad. Por ejemplo, la ciudad de Taiyuan, en China, la primera en la lista con una

prevalencia de 119,57 cámaras por cada 1.000 habitantes tiene un índice de delincuencia de 51,47%. “En términos generales, más cámaras no necesariamente reducen las tasas de criminalidad”. Este dato no solo es importante para cuestionar la relación entre la vigilancia y la seguridad. Esta información le interesa a la Corte Constitucional, porque afecta la evaluación de la necesidad e idoneidad de la medida objeto de control en el marco del juicio de proporcionalidad propuesto. En este sentido, confirma también los hallazgos hechos por la Corporación en decisiones anteriores.

313. La Corte también ha constatado en varios de sus pronunciamientos que no hay prueba fehaciente de la necesidad o idoneidad de la medida, esto es, que no existen elementos de convicción dirigidos a confirmar que el acceso de la Policía Nacional a circuitos cerrados de vigilancia y seguridad privada para acciones de prevención –que la propia ley se abstiene de definir, precisar y acotar– contribuya, en efecto, a disminuir la delincuencia –se destaca–.

314. En la sentencia T-407 de 2012 –a la que se hizo referencia–, la Corte dejó claro que estas medidas de videovigilancia representan una injerencia profunda en los derechos fundamentales a la intimidad y al hábeas data, así como en relación con otros derechos fundamentales cuya protección se encuentra estrechamente relacionada con el debido cumplimiento de aquellos. Es más, la Corporación indicó que no se había constatado que existiera un vínculo de causalidad comprobado entre la instalación de sistemas de videovigilancia y seguridad con la disminución o aumento de las conductas delictivas –se destaca–. En esa oportunidad precisó, igualmente, que, si bien la medida podía ayudar, no había estudios “que sustenten más allá de la percepción de la gente, la real disminución de la violencia o los hechos delictivos como consecuencia de la instalación de cámaras de seguridad”.

315. La inexistencia de una relación directa entre el aumento de la vigilancia y el aumento de la seguridad también impacta la proporcionalidad en sentido estricto de la medida objeto de examen –se destaca–. Lo anterior, por cuanto el sacrificio de los derechos fundamentales

puestos al otro lado de la balanza no está directamente relacionado con un beneficio correlativo directo en materia de seguridad. Eso significa que habría un alto sacrificio de varios derechos y libertades fundamentales sin que ello comporte necesariamente un beneficio para otros derechos constitucionales.

316. En fin, la Sala observa que las posibles ventajas que eventualmente podrían obtenerse en materia de seguridad con lo dispuesto en la norma acusada en relación con la potestad atribuida a la Policía Nacional con el objeto de que acceda a circuitos cerrados de vigilancia y seguridad privada “para acciones de prevención”, resultan desmedidas cuando se repara en la profunda injerencia que deben soportar los derechos fundamentales a la intimidad y al hábeas data intervenidos, sacrificio que, a la luz de la importancia que el ordenamiento nacional e internacional le confieren a estos derechos fundamentales, no resulta de manera alguna compensable con una incierta ventaja de la seguridad colectiva. Brevemente, la Corte constata una dudosa conexión entre los propósitos de vigilancia y seguridad para acciones de “prevención” de la norma acusada y la efectiva consecución de estos fines -se destaca-.

317. Teniendo en cuenta las razones desarrolladas, la Sala considera que en este caso la facultad otorgada a la Policía Nacional con el objeto de acceder a circuitos cerrados de vigilancia y seguridad privada para acciones de “prevención” es contraria a los artículos 15 de la Carta Política , 12 de la Declaración Universal de los Derechos Humanos , 11 de la Convención Americana sobre Derechos Humanos , 17 del Pacto Internacional de Derechos Civiles y Políticos y 4º , 5º y 6º de la Ley Estatutaria 1581 de 2012 “por la cual se dictan disposiciones generales para la protección de datos personales”. Por esa razón, en la parte resolutive de la presente sentencia declarará la inexecutable de la expresión “prevención” contemplada en la norma demandada.

b) Examen de la facultad que la norma acusada le otorga a la Policía Nacional de acceder a circuitos cerrados de seguridad y vigilancia privados para acciones de identificación y judicialización

318. ¿Qué sucede entretanto con la facultad que la disposición acusada otorgó a la Policía Nacional con el fin de que acceda a circuitos cerrados de seguridad y vigilancia privada para acciones de identificación y judicialización? Respecto de esta atribución, ¿incurrió el Legislador en una omisión legislativa relativa?

Para responder ese interrogante, también debe aplicarse, previamente, la herramienta hermenéutica de la ponderación y, de este modo, resulta necesario evaluar la razonabilidad y proporcionalidad de la medida.

319. Primeramente, es de advertir, que las acciones de identificación y judicialización se encuentran estrechamente relacionadas entre sí. La identificación resulta a toda luz indispensable en el proceso de imputación o judicialización y su práctica en este caso se debe circunscribir o vincular con una investigación penal en curso lo que acota, de manera más precisa y clara, su ámbito de aplicación y evita o disminuye considerablemente los excesos que podrían presentarse –se destaca–. Así, salvo que tengan lugar irregularidades que habrían de ser examinadas en cada caso concreto, las acciones de identificación y judicialización se sujetan a las regulaciones procesales y sustantivas derivadas del ordenamiento jurídico, como se expuso detalladamente en las consideraciones de la presente sentencia.

320. Además, la facultad otorgada a la Policía Nacional – en su rol de Policía Judicial– con el objeto de que acceda a circuitos cerrados de seguridad y vigilancia privada para acciones de identificación y judicialización encuentra una justificación constitucional válida e incluso imperiosa cuando se presenta en el marco de un proceso penal bajo la instrucción y coordinación de la Fiscalía General de la Nación –se destaca–.

321. Arriba se mencionó que perseguir y sancionar conductas que atentan contra personas y bienes puede calificarse como una razón suficiente y constitucionalmente válida e, incluso,

imperiosa para restringir los derechos fundamentales a la intimidad y al hábeas data. No obstante, también se mostró cómo la jurisprudencia constitucional ha sido enfática en que esto solo puede suceder cuando existe una regulación legal y autorización judicial previa –se destaca-. Igualmente, se resaltó que, en caso de flagrancia o de actos urgentes, la intervención judicial puede ser posterior –se destaca-.

322. Es claro para la Sala que atribuir a las dependencias especializadas de la Policía Nacional en su rol de Policía Judicial la facultad de acceder a circuitos cerrados de vigilancia y seguridad privada para acciones de identificación y judicialización –acorde con lo dispuesto en el artículo 201 de la Ley 906 de 2004-, cumple con las exigencias de claridad, precisión y determinación de la medida, por lo que el riesgo de exceso o arbitrariedad se restringe o no se presenta.

323. En segundo lugar, la propia jurisprudencia constitucional ha reconocido que, entre los aspectos que pueden llegar a restringir los derechos fundamentales, se encuentra “el interés de la sociedad de que se investiguen las conductas delictivas y se sancione a los responsables, en procura de preservar la vigencia de un orden justo”.

324. Al respecto debe recordarse, igualmente, que el acceso a la información por parte de las autoridades no está vedado en todos los casos. Así, tratándose de información de carácter público no puede existir reserva y lo que prima es el principio de máxima divulgación. No sucede lo mismo con información personal que incluye datos sensibles, pues se entiende que esta es información reservada no sujeta a divulgación por estar vinculada con el núcleo esencial de los derechos a la libertad, dignidad e intimidad de su titular. En estos casos, la información solo puede ser accesible en tanto medie su consentimiento. Es de destacar que este tipo de información permanece resguardada incluso en lugares públicos, semi públicos o semi privados.

325. En ese sentido y, como quedó referido en las consideraciones de la presente sentencia, la Corte ha puntualizado que está vedado el acceso a la información reservada, esto es, la que equivale a datos sensibles y del interés exclusivo y excluyente de su titular –estrechamente relacionada con la protección de sus derechos fundamentales a la dignidad humana, a la intimidad, al libre ejercicio de la personalidad–. Sin embargo, la jurisprudencia también ha reconocido una salvedad: que el dato objeto de reserva constituya “un elemento probatorio pertinente y conducente dentro de una investigación penal” y que este se relacione de manera directa con el objeto de la investigación.

326. En tercer lugar, la Corte ha enfatizado en que acopiar “información en relación con las personas investigadas puede ser eventualmente un medio necesario para cumplir con el mencionado propósito, pero igualmente ha insistido en la necesidad de que el recaudo de pruebas se lleve a cabo “con escrupuloso acatamiento de las previsiones que la propia Constitución ha establecido para la protección de los derechos fundamentales especialmente expuestos a su afectación, vulneración o mengua en el contexto de una investigación criminal”.

327. Como se advirtió, la Corte ha destacado que la tarea central de los organismos de vigilancia y control estatal –entre estos la Policía Nacional–, debe sujetarse a los controles existentes y no pasarlos por alto. Ha insistido en que los procedimientos policiales deben realizarse “dentro del estricto respeto por los derechos humanos”. En criterio de la Corte, de ello depende no sólo la seguridad ciudadana y la legitimidad de la acción de las autoridades sino, incluso, la propia eficacia de la investigación y sanción de los delitos”. La Corporación ha resaltado cómo “la sociología criminal ha mostrado que la eficacia en la lucha contra el delito depende en gran parte de la confianza que la población tenga en las autoridades, la cual deriva del actuar conforme a los derechos humanos”.

328. Adicionalmente, cabe traer a colación la intervención del Ministerio de Justicia y del Derecho que, tras nombrar los artículos 15 y 250 superiores y la Ley Estatutaria de

Protección de Datos Personales, puso especial énfasis en que para que la Policía Nacional acceda a información personal captada por medio de sistemas de seguridad y vigilancia para fines de judicialización –al margen del lugar en el que estas se encuentren localizadas–, resulta indispensable contar con autorización judicial previa cuando puedan verse afectados derechos fundamentales como el derecho a la intimidad y al hábeas data –se destaca–. Con el fin de acceder a esta información deben cumplirse, además, los principios relativos a la protección de datos previstos en el artículo 4º de la Ley Estatutaria 1581 de 2012 y aquellos desarrollados por la jurisprudencia constitucional.

330. Sin embargo, al no haber establecido la disposición acusada en forma expresa la necesidad de autorización –previa o posterior–, por la autoridad judicial competente, resulta contraria al ordenamiento, al tiempo que desconoce la jurisprudencia constitucional, generando una desproporción que vulnera abiertamente los derechos a la intimidad y al hábeas data contemplados en el artículo 15 superior y en el régimen general de tratamiento de datos personales –Ley Estatutaria 1581 de 2012–.

331. Por eso, la Sala concluye que le cabe razón al accionante en el sentido de que, en relación con el supuesto de la norma acusada que autoriza el acceso de la Policía Nacional a circuitos cerrados de vigilancia y seguridad privada para acciones de identificación y judicialización, el Legislador efectivamente incurrió en una omisión legislativa relativa, sin que medie justificación constitucional alguna –se destaca–. Esta omisión se hace clara cuando se toma en cuenta la normatividad constitucional y legal vigente, tanto como la jurisprudencia que sobre la materia ha proferido la Corte Constitucional, de la que se dejó constancia en las consideraciones de la presente providencia.

332. Al respecto es de anotar cómo la Corporación ha destacado que, únicamente, las autoridades especialmente capacitadas para el efecto y “no toda la Policía Nacional, ni todos

los integrantes del Cuerpo Técnico de Investigación de la Fiscalía General de la Nación” están en condición de desempeñar funciones de policía judicial –se destaca–.

333. Como quedó expuesto, estas funciones solo pueden ser desarrolladas por “quienes constituyan dentro de las entidades respectivas un cuerpo especial: el de “policía judicial”. Adicionalmente ha especificado que, acorde con lo dispuesto en el numeral 3º del artículo 250 superior, le corresponde a la Fiscalía General de la Nación dirigir y coordinar las funciones de policía judicial que en forma permanente cumplen la Policía Nacional y los demás organismos que señale la ley.

334. En este sentido puede concluirse que las facultades concedidas a la Policía Nacional para obrar como Policía Judicial –y en ese marco preciso adelantar acciones de identificación o judicialización–, se encuentran ajustadas al ordenamiento siempre que, según lo dispuesto en el numeral 3º del artículo 250 superior, obtengan autorización judicial previa cuando las acciones de investigación afecten derechos fundamentales, tales como los derechos a la intimidad y al hábeas data –se destaca–. En casos de flagrancia o de acciones urgentes, la intervención judicial puede ser posterior, como quedó dicho en las consideraciones de la presente sentencia –se destaca–.

335. Tal previsión fue omitida por el Legislador en la disposición acusada, pese a la severa injerencia que de lo allí consignado se puede derivar, tanto frente al derecho a la intimidad personal y familiar del titular, como respecto de su derecho fundamental al hábeas data a raíz de las medidas de identificación o judicialización conferidas a la Policía Nacional. Así, se omitió injustificadamente la necesaria autorización –previa o posterior–, de la autoridad judicial competente, única forma de preservar el núcleo esencial de estos derechos fundamentales y el manejo adecuado de datos personalísimos.

336. Como consecuencia de la configuración de esta omisión legislativa relativa, la Corte

modulará el contenido de su sentencia y, en esa medida, incorporará a la disposición acusada los elementos que el legislador excluyó injustificadamente.

En tal virtud, el artículo 48 de la Ley 2197 “por medio de la cual se dictan normas tendientes al fortalecimiento de la seguridad ciudadana y se dictan otras disposiciones”, será declarado exequible y continuará en el ordenamiento jurídico bajo el siguiente condicionamiento: en el entendido de que los integrantes de la Policía Nacional que ejercen funciones de Policía Judicial, podrán acceder a los circuitos cerrados de vigilancia y seguridad privada para acciones de identificación o judicialización en el marco de una investigación de carácter penal, previa autorización de la autoridad judicial correspondiente, salvo en los actos urgentes, los casos de flagrancia y en otras actuaciones que no requieren autorización judicial previa para su realización. Esto, acorde con la normativa procesal penal y los principios que rigen la protección de datos personales.

11. Síntesis de la decisión

337. Al fijar el alcance de la disposición acusada, la Sala indicó que esta facultó a la Policía Nacional para efectuar el manejo de datos personales en dos sentidos. Primero, para acceder a la información consignada en circuitos cerrados de vigilancia y seguridad privada y, segundo, para usar los datos allí registrados, con el propósito de ejecutar acciones de prevención, identificación o judicialización. La Sala encontró que en los dos supuestos descritos la atribución conferida a la mencionada autoridad fue absoluta, esto es, no se encuentra sujeta a condición o requerimiento alguno.

338. Teniendo en cuenta el sentido y alcance del artículo 48 de la Ley 2197 de 2022, le correspondió a la Sala establecer si el Legislador al expedir la norma acusada que i) permitió el acceso irrestricto de la Policía Nacional a circuitos cerrados de vigilancia y seguridad privada en la que datos de personas determinadas o indeterminadas quedan almacenados o

registrados y, además, ii) facultó a esta autoridad para el uso también incondicionado de estos datos con el propósito de ejecutar acciones de prevención, identificación o judicialización, ¿habría incurrido en una omisión legislativa relativa desconociendo los derechos fundamentales a la intimidad y al hábeas data (protección de datos personales) y, en ese sentido, estaría vulnerando los artículos 15 de la Carta Política, 12 de la Declaración Universal de los Derechos Humanos, 17 del Pacto Internacional de Derechos Civiles y Políticos, así como 4º, 5º, y 6º de la Ley Estatutaria 1581 de 2012?

339. Con el objetivo de resolver el problema jurídico, la Sala trajo a colación su jurisprudencia en relación con los derechos fundamentales a la intimidad y al hábeas data. Además, reiteró sus pronunciamientos en torno a las fronteras constitucionales y legales a las que se sujeta la Policía Nacional como Policía Judicial y las limitaciones que ha trazado el ordenamiento jurídico a las empresas privadas que prestan el servicio de vigilancia y seguridad.

340. De otro lado, se pronunció respecto de la tecnología vinculada con circuitos cerrados de vigilancia y seguridad privada, así como sobre su regulación jurídica. Igualmente, se refirió a los criterios fijados por la jurisprudencia constitucional para ponderar el conflicto entre, por un lado, la seguridad y la vigilancia y, por el otro, los derechos fundamentales a la intimidad y al hábeas data –cuya vigencia se relaciona, estrechamente, con la necesidad de respetar la dignidad humana, la libertad y la autonomía de las personas–. Finalmente, realizó el examen de constitucionalidad de la norma acusada.

341. Ahora bien, antes de evidenciar si, como lo alegó el demandante, el Legislador incurrió en una omisión legislativa relativa, la Sala consideró importante efectuar un análisis separado de las acciones para las cuales la norma acusada facultó a la Policía Nacional y, de esta manera, encontró indispensable indagar sobre la proporcionalidad de estas medidas. En primer lugar, examinó si la atribución asignada por la norma a la Policía Nacional para acciones de “prevención” podía considerarse proporcionada en sentido estricto.

342. Con ese propósito, reiteró que, si es cierto que el tratamiento de datos mediante circuitos cerrados de seguridad y vigilancia privada podría tener efectos disuasivos en el conglomerado social para la protección de personas y bienes, también lo es que este desarrollo tecnológico podría estar en condición de lesionar derechos fundamentales. De ahí que el ordenamiento nacional y los tratados internacionales sobre derechos humanos hayan establecido un conjunto de principios para la administración de datos personales que deben ser aplicados –de manera estricta– al momento de ponderar derechos y bienes jurídicos en tensión y, de esta forma, evitar el ejercicio “abusivo y arbitrario de la libertad informática”.

343. En fin, la Corte consideró que la facultad otorgada a la Policía Nacional de acceder a circuitos cerrados de seguridad y vigilancia privada para acciones de “prevención” era desproporcionada. En primer lugar, por la indeterminación absoluta de la medida que, dados los alcances de la tecnología usada que avanza de manera vertiginosa, impide asegurar que el uso de esta técnica se mantenga dentro de los cauces constitucionales, legales y reglamentarios que son los que permiten salvaguardar el núcleo esencial de los derechos fundamentales en juego.

344. De otra parte, la Sala reiteró que “[e]l derecho a la intimidad siempre mantiene una esfera de protección por su naturaleza ontológica”. Esto significa que, pese a que la expectativa de privacidad puede variar e incluso las personas –en aras de disuadir a la delincuencia y de proteger a personas y a bienes–, pueden consentir en la instalación de videocámaras de vigilancia y seguridad en lugares privados, la regulación constitucional de los derechos fundamentales a la intimidad y al hábeas data, así como la ordenación legal y reglamentaria que la desarrolla muestra que, incluso en espacios públicos, pero, con mayor razón, en espacios privados se debe mantener un grado de garantía de la intimidad personal y familiar, tanto como de los datos sensibles. Además, expuso los motivos por los cuales esta exigencia sería imposible de aplicar en un escenario como el que plantea la disposición demandada, en punto a la potestad conferida a la Policía Nacional para acciones de “prevención”.

345. La Sala encontró que cuando la disposición demandada faculta a la Policía Nacional con el objeto de que acceda a los archivos de video en los que están contenidos los datos de personas determinadas o indeterminadas para acciones de “prevención”, no solo está poniendo a disposición de la Policía Nacional imágenes. También habilita a esta autoridad para que se aproxime a otra información personalísima que es igualmente sensible.

346. En síntesis, la Sala consideró que la potestad conferida a la Policía Nacional en la norma acusada para acciones de “prevención” aun cuando podría dar, inicialmente, la sensación de protección a personas y a bienes y, en tal sentido, tener un efecto disuasivo frente a la delincuencia, resulta desproporcionada, habida cuenta de que no existe prueba fehaciente de la necesidad o idoneidad de la medida, pues no hay certeza alguna de que el acceso de la mencionada autoridad a circuitos cerrados de vigilancia y seguridad privada con el propósito de ejecutar acciones de “prevención” –que la propia ley se abstiene de definir, precisar y acotar– contribuya, en efecto, a disminuir conductas delictivas. En suma, la Corte constató una dudosa conexión entre los propósitos de vigilancia y seguridad para acciones de “prevención” de la norma acusada y la efectiva consecución de estos fines.

347. En el sentido expresado, la Sala precisó que las ventajas que, eventualmente, podrían obtenerse en materia de seguridad con lo dispuesto en la norma acusada a propósito de las acciones de “prevención” concedidas a la Policía Nacional, no se encontraban en relación de proporcionalidad estricta con la profunda injerencia que deben soportar los derechos fundamentales intervenidos, sacrificio que, a la luz de la importancia que el ordenamiento nacional e internacional le confieren a los derechos fundamentales a la intimidad personal y familiar, como al hábeas data, no resulta de manera alguna compensable con una incierta ventaja de la seguridad colectiva.

348. Por los motivos expuestos resolvió declarar inexecutable el término “prevención”

contemplado en la norma acusada.

349. En relación con las expresiones “identificación” o “judicialización”, la Corporación las encontró ajustadas al ordenamiento, en la medida en que se apliquen dentro del marco de una investigación de carácter penal, bajo la dirección y coordinación de la Fiscalía General de la Nación, como lo dispone el ordenamiento jurídico y lo ha reiterado la Corte Constitucional.

350. De esta manera, compartió la tesis expuesta por el demandante, en el sentido de que, efectivamente, el legislador al redactar la disposición acusada incurrió en una omisión legislativa relativa, pues, pasó por alto, sin existir motivo constitucionalmente válido, la necesidad de sujetar la facultad atribuida en la norma acusada a la Policía Nacional para acciones de “identificación” o “judicialización” a unas condiciones que la acoten y sujeten a las previsiones constitucionales, legales y reglamentarias. En tal virtud, la Corte ordenó modular el contenido de la sentencia y dispuso incorporar a la disposición los elementos que el Legislador excluyó injustificadamente.

351. Acto seguido, la Sala puntualizó que la atribución prevista en el artículo 48 de la Ley 2197 de 2022 demandado de acceder a circuitos privados de seguridad y vigilancia privada para acciones de “identificación” o “judicialización” no se asigna a la Policía Nacional, en general, sino, concretamente, a la Policía Judicial, autoridad que podrá acceder a estos circuitos en el marco de una investigación de carácter penal, previa autorización de la autoridad judicial correspondiente, salvo en los actos urgentes, los casos de flagrancia y en otras actuaciones que no requieren autorización judicial previa para su realización. Esto, acorde con la normativa procesal penal y los principios que rigen la protección de datos personales.

III. DECISIÓN

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

RESUELVE:

PRIMERO.- Declarar INEXEQUIBLE la expresión “prevención” establecida en el artículo 48 de la Ley 2197 de 2022 “por medio de la cual se dictan normas tendientes al fortalecimiento de la seguridad ciudadana y se dictan otras disposiciones”.

SEGUNDO.- Declarar EXEQUIBLE el artículo 48 de la Ley 2197 de 2022, en el entendido de que los integrantes de la Policía Nacional que ejercen funciones de Policía Judicial, podrán acceder a los circuitos cerrados de vigilancia y seguridad privada para acciones de identificación o judicialización en el marco de una investigación de carácter penal, previa autorización de la autoridad judicial correspondiente, salvo en los actos urgentes, los casos de flagrancia y en otras actuaciones que no requieren autorización judicial previa. para su realización. Esto, acorde con la normativa procesal penal y los principios que rigen la protección de datos personales.

Notifíquese, comuníquese y cúmplase.

CRISTINA PARDO SCHLESINGER

Presidenta

NATALIA ÁNGEL CABO

Magistrada

DIANA FAJARDO RIVERA

Magistrada

Magistrado

ALEJANDRO LINARES CANTILLO

Magistrado

Con aclaración de voto

ANTONIO JOSÉ LIZARAZO OCAMPO

Magistrado

Con salvamento parcial de voto

PAOLA ANDREA MENESES MOSQUERA

Magistrada

HERNÁN CORREA CARDOZO

Magistrado (E)

Con aclaración de voto

JOSE FERNANDO REYES CUARTAS

Magistrado

Con aclaración de voto

MARTHA VICTORIA SÁCHICA MÉNDEZ

Secretaria General

SALVAMENTO PARCIAL DE VOTO DEL MAGISTRADO

A LA SENTENCIA C-406/22

Referencia: Expediente D-14.799

Con el acostumbrado respeto por las decisiones de la Corte Constitucional, salvo parcialmente mi voto en relación con la declaratoria de inexecuibilidad de la expresión “prevención”, contenida en el artículo 48 de la Ley 2197 de 2022, que adicionó el artículo 237B a la Ley 1801 de 2016 Código Nacional de Seguridad y Convivencia Ciudadana, y con

los términos en que se condicionó el contenido normativo restante de esta disposición, por las siguientes tres razones, a partir de las cuales considero que no es posible atribuir a la norma el contenido que le imputó la mayoría de la Sala:

1. En primer lugar, la norma regula un medio adicional al que se ordena en el artículo 237 de la Ley 1801 de 2016 para el acceso a los sistemas y circuitos de vigilancia privados, y, a diferencia de esta última disposición, lo hace para tres fines específicos: “prevención”, “identificación” y “judicialización”, todos tendientes al cumplimiento de una finalidad constitucionalmente relevante, que se relaciona con la protección de los derechos y libertades de los colombianos a cargo de la Policía Nacional. En efecto, mientras que el artículo 237 de la Ley 1801 de 2016 regula la “integración de sistemas de vigilancia” mediante su “enlace” “permanente o temporal a la red que para tal efecto disponga la Policía Nacional” y sin que la norma lo adscriba al ejercicio de alguna función específica de dicho órgano, el artículo 237B regula un medio adicional, que se relaciona con la facultad de “acceder” a “circuitos cerrados de vigilancia y seguridad privada” para ejercer las funciones de “prevención”, “identificación” o “judicialización” a cargo de la Policía Nacional.

2. En segundo lugar, en atención a esta relación de complementariedad, las acciones de “prevención”, “identificación” y “judicialización” previstas en el artículo 237B deben interpretarse de manera armónica con el contenido del artículo 237 que le precede y con sujeción a las exigencias previstas en el condicionamiento del que este artículo fue objeto en la Sentencia C-094 de 2020, mediante la cual se declaró condicionalmente exequible el artículo 237 de la Ley 1801 de 2016.

La Corte señaló en dicha sentencia que la instalación de cámaras de vigilancia en lugares semiprivados y semipúblicos no resulta, en principio, inconstitucional, siempre y cuando su instalación atienda el contenido de los principios de finalidad, necesidad y proporcionalidad. De allí que la posibilidad de instalar cámaras de video en este tipo de espacios semipúblicos sea admisible, dado que “hay mayor tolerancia al control y vigilancia sobre las conductas de

las personas con el fin de evitar y prevenir situaciones de riesgo ya que las repercusiones sociales son mayores”.

En esa línea, también se indicó en la citada providencia que la instalación de cámaras de video vigilancia en espacios públicos que se integran permanentemente a circuitos cerrados de televisión controlados y monitoreados por autoridades constituye una herramienta idónea para la prevención y persecución del delito. De allí que hubiese considerado que el artículo 237 de la Ley 1801 de 2016 persigue una finalidad constitucionalmente legítima que consiste en prevenir el crimen y promover la seguridad ciudadana, por lo que “si bien podría afectarse eventualmente el comportamiento de las personas y su expectativa de privacidad en los sitios señalados por la norma demandada, no se puede desconocer el beneficio en materia de seguridad, interés general y protección del orden público”.

De lo dicho se sigue que la Policía Nacional está facultada para acceder a los sistemas y circuitos de vigilancia privada con la finalidad de “prevenir” y para ejercer las funciones de “identificación” y “judicialización” (de que trata el artículo 237B – que se demanda), siempre que estas se realicen en los mismos términos del condicionamiento previsto en la Sentencia C-094 de 2020 respecto del artículo 237 de la Ley 1801 de 2016, es decir, en el entendido de que “la captación y/o almacenamiento de información, datos o imágenes a los que se refiere la norma acusada deberá ceñirse en todo momento a los principios establecidos en la Ley 1581 de 2012, en especial, la determinación del tiempo de conservación de la información, las obligaciones de tratamiento de la misma, y las personas entre las cuales se puede circular”. De allí que no es acertada la declaratoria de inexecutable de la expresión “prevención”, contenida en el artículo 48 de la Ley 2197 de 2022, que adicionó el artículo 237B a la Ley 1801 de 2016, y tampoco adecuado el alcance del condicionamiento de que fue objeto el restante contenido normativo de la disposición.

3. Finalmente, en relación con cada una de las funciones que le asigna la disposición acusada a la Policía Nacional, lo cierto es que (i) el acceso a circuitos cerrados de vigilancia y

seguridad privada para realizar acciones de “prevención” debe entenderse en el sentido de que este no comprende las grabaciones que se realicen en el ámbito exclusivamente personal o domiciliario, y; (ii) las acciones de “identificación” y “judicialización” (a) no pueden limitarse al concepto de “investigación”, sino que deben entenderse referidas al “proceso o actuación de carácter penal”, y (b) no es adecuado condicionar la exequibilidad de la norma a que el acceso de la Policía Nacional a los sistemas y circuitos de videovigilancia cuente con “previa autorización por parte de la autoridad judicial correspondiente”.

En relación con lo primero, los “circuitos cerrados de vigilancia y seguridad privada” a que hace referencia la disposición que se demanda deben entenderse referidos a los empleados en la prestación del servicio de vigilancia y seguridad privada, en los términos dispuestos por el Decreto Ley 356 de 1994 (“por el cual se expide el estatuto de vigilancia y seguridad privada”). Por tanto, esta atribución de competencia a favor de la Policía Nacional no comprende el acceso a las grabaciones que se realicen en el ámbito exclusivamente personal o domiciliario.

De un lado, el artículo 5 del Decreto Ley 356 de 1994 dispone que entre los “medios para la prestación de los servicios de vigilancias y seguridad privada” se pueden utilizar mecanismos tecnológicos o cualquier otro medio autorizado por la Superintendencia de Vigilancia y Seguridad Privada. En este sentido, la “Guía de Protección de Datos Personales en Sistemas de Videovigilancia de la Superintendencia de Industria y Comercio” prevé que los sistemas de videovigilancia o cámaras de seguridad constituyen métodos de vigilancia a través de un sistema de cámaras, fijas o móviles, que no se extienden respecto de las grabaciones que se realicen dentro del ámbito exclusivamente personal o doméstico.

De otro lado, el objetivo del servicio de vigilancia y seguridad privada es “disminuir y prevenir las amenazas que afecten o puedan afectar la vida, la integridad personal o el tranquilo ejercicio de legítimos derechos sobre los bienes de las personas que reciben su

protección, sin alterar o perturbar las condiciones para el ejercicio de los derechos [y] libertades públicas de la ciudadanía sin invadir la órbita de competencia reservada a las autoridades” (artículo 73 del Decreto Ley 356 de 1994). Y uno de los principios que rige la prestación de este servicio es el de contribuir a la prevención del delito (artículo 74, numeral 6, del Decreto Ley 356 de 1994).

De un lado, circunscribir el acceso de la Policía Nacional a los circuitos cerrados de vigilancia y seguridad privada para realizar acciones de “identificación” o “judicialización” desconoce la posibilidad de que la autoridad ejerza estas acciones en otros ámbitos del proceso penal diferentes a la investigación, en las que, de acuerdo con la legislación procesal penal, sería viable recaudar otros elementos de prueba para constatar la efectiva comisión de delitos. Esta diferencia es especialmente relevante, además, si se tiene en cuenta que la disposición es aplicable no solo al procedimiento penal regido por la Ley 906 de 2004, sino al regulado por la Ley 600 de 2000.

De otro lado, condicionar la actividad de la Policía Nacional a la autorización previa de la autoridad judicial competente limita la función de “3. Prevenir situaciones y comportamientos que ponen en riesgo la convivencia”, de que trata el artículo 10 de la Ley 1801 de 2016. Además, dado que la disposición que se demanda regula un supuesto de “acceso” “a los circuitos cerrados de vigilancia y seguridad privada” (artículo 237B) cuando no se cuente con el “enlace” “permanente o temporal a la red que para tal efecto disponga la Policía Nacional” respecto de los “sistemas de vigilancia” (artículo 237), es posible entender que las acciones de “identificación” y “judicialización” debían sujetarse al mismo condicionamiento de la primera disposición, en los términos de Sentencia C-094 de 2020.

De allí que someter el ejercicio de estas funciones a la previa autorización judicial restringe considerablemente el fin constitucional adscrito a la función de la Policía Nacional: “el

mantenimiento de las condiciones necesarias para el ejercicio de los derechos y libertades públicas, y para asegurar que los habitantes de Colombia convivan en paz” (artículo 218 de la Constitución), y desconoce que el artículo 14 de la Ley 906 de 2006 protege el derecho a la intimidad que con el condicionamiento se buscó, pues dicha disposición establece que “No podrán hacerse registros, allanamientos ni incautaciones en domicilio, residencia, o lugar de trabajo, sino en virtud de orden escrita del Fiscal General de la Nación o su delegado, con arreglo de las formalidades y motivos previamente definidos en este código”, no obstante lo cual excluía de dicha orden escrita las situaciones de flagrancia y demás contempladas por la ley (resalto propio).

ANTONIO JOSÉ LIZARAZO OCAMPO

Magistrado

ACLARACIÓN DE VOTO DEL MAGISTRADO

JOSÉ FERNANDO REYES CUARTAS

SENTENCIA C-406/22

1. 1. Con el debido respeto por las determinaciones de la Sala Plena de la Corte Constitucional, presento las razones de mi aclaración de voto a la Sentencia C-406 de 2022. Esa decisión declaró la inconstitucionalidad de la expresión “prevención” establecida en el artículo 48 de la Ley 2197 de 2022 y la constitucionalidad condicionada de ese mismo artículo:

“(...) en el entendido de que los integrantes de la Policía Nacional que ejercen funciones de Policía Judicial, podrán acceder a los circuitos cerrados de vigilancia y seguridad privada para acciones de identificación o judicialización en el marco de una investigación de carácter penal, previa autorización de la autoridad judicial correspondiente, salvo en los actos urgentes, los casos de flagrancia y en otras actuaciones que no requieren autorización judicial previa”.

2. Acompañé la decisión de la Sala Plena. Sin embargo, creo que el argumento mayoritario ha debido profundizar en los diques al poder de vigilancia del Estado a través de los mecanismos electrónicos y, en especial, de la videovigilancia. Me preocupa el hecho de que la proliferación de los dispositivos de captación de la imagen en todo el mundo es una tendencia hacia una sociedad videovigilada. La región latinoamericana no escapa de esa tendencia tanto si se la evalúa por el número de dispositivos como por la densidad de cámaras en relación con los kilómetros cuadrados.

3. De manera que la intención de aprovechar este tipo de tecnología para fomentar la seguridad ha llevado a que se construyan redes de vigilancia civil remuneradas y portales web en los que se ofrece dinero para que los ciudadanos monitoreen los circuitos cerrados de televisión (en adelante CCTV). Se les denomina el paraíso de los fisgones. Pero ciertamente esa expresión no es sino un eufemismo para lo que, en realidad, es una sociedad de la vigilancia y del control. Es innegable que hay muchas ventajas que derivan de la proliferación

de estos dispositivos (i.e. facilidad probatoria, protección de víctimas o auto-restricción de las autoridades de policía que usan las boby cams). Pero creo que nos correspondía dejar sentadas algunas premisas sobre sus inmensos riesgos para las libertades ciudadanas.

4. En especial, considero pertinentes cinco reflexiones para limitar el uso tanto de esas facultades de acceso a los CCTV por parte de la Policía como de la información que de allí se obtenga.

1. La dudosa conexión entre la vigilancia y la seguridad

5. En primer lugar, pienso que era necesario evaluar la necesidad e idoneidad de las medidas revisadas por la Sala Plena de conformidad con la muy dudosa relación entre la vigilancia y la seguridad. Esta conexión no ha sido nunca directamente proporcional. En efecto, no es necesariamente cierto que a mayor grado de vigilancia habrá un mayor grado de seguridad. Esa relación no ocurría en Foucault y no ocurre ahora en 2022. Como demuestran algunas de las cifras sobre las ciudadanes más videovigiladas del mundo:

“La tecnología de reconocimiento facial hace posible que tanto las entidades públicas como las privadas verifiquen instantáneamente la identidad de cualquier persona que pase por una cámara CCTV. || Sin embargo, los resultados de esta investigación no mostraron una relación que confirme la relación entre vigilancia y mayor seguridad. Encontraron poca correlación entre la cantidad de cámaras CCTV públicas y el crimen o la seguridad. Por ejemplo, la ciudad de Taiyuan, en China, la primera en la lista con una prevalencia de 119,57 cámaras por cada 1.000 habitantes tiene un índice de delincuencia de 51,47%. “En términos generales, más cámaras no necesariamente reducen las tasas de criminalidad”.

6. El anterior dato no solo es importante para cuestionar la relación entre la vigilancia y la seguridad. Esta información le interesaba a la Corte Constitucional porque impactaba la evaluación de la necesidad e idoneidad de la medida que era objeto de control en el marco de un juicio de proporcionalidad. De manera que este es un principio que me parece claro y que debió quedar registrado en nuestra decisión: la videovigilancia es un mecanismo, pero no es el único, ni mucho menos el mejor, para lograr los fines de prevención, identificación o judicialización que llevaron al legislador a proferir esa habilitación a favor de la Policía.

7. La inexistencia de una relación directa entre el aumento de la vigilancia y el aumento de la seguridad también impacta la proporcionalidad en sentido estricto de este tipo de medidas. El sacrificio para las libertades que la medida representa no está directamente relacionado con un beneficio correlativo directo en materia de seguridad. Eso significa que habría un alto sacrificio de varias libertades (i.e. intimidad, habeas data, privacidad) sin que ello representara necesariamente un beneficio para otros derechos constitucionales.

8. La conclusión constitucional de mi primera reflexión es que la aplicación del juicio de proporcionalidad a la norma objeto de control debió tener en cuenta una visión crítica de la eficacia de estos mecanismos para lograr los fines propuestos. Esos objetivos pretenden justificar la existencia de la habilitación a la Policía para acceder a los CCTV. Sin embargo, existen muchas dudas sobre la conducencia de esa limitación a los derechos constitucionales para lograr esos beneficios. De allí que la presunción de constitucionalidad de ese tipo de medidas sea menor y la carga argumentativa necesaria para mantenerlas dentro del ordenamiento debiera ser muy exigente.

2. Era imprescindible acotar los objetivos o fines que justifican el acceso a la videovigilancia

9. En segundo lugar, me interesa señalar que los objetivos de la videovigilancia debieron quedar muy bien acotados. Eso era imprescindible para la legitimidad de ese mecanismo en

un Estado que se rige por las libertades ciudadanas y que evita la instrumentalización de los individuos. Por eso quiero señalar que la regulación alemana limita la videovigilancia en los espacios públicos a tres finalidades expresas: “1. para el cumplimiento de funciones de entidades públicas, 2. para el ejercicio de las facultades de policía dentro de los edificios o 3. para la salvaguarda de intereses legítimos con fines concretamente establecidos”.

10. La premisa es que la videovigilancia en los espacios públicos solo es permitida bajo ciertas finalidades. Si la videovigilancia en espacios públicos aparece bien limitada por esos propósitos, pienso que asisten mayores argumentos para limitar los objetivos que justifican el acceso de la Policía a la videovigilancia privada. Como es bien sabido, la intimidad no tiene que desaparecer en cuanto salimos de nuestros domicilios. Por eso el Estado no nos puede vigilar en la calle o en los espacios públicos por cualquier razón o de cualquier manera. Cuando se trata de los CCTV privados, existen mayores razones para indicar que debe prevalecer el derecho a la intimidad.

11. Como este tribunal ha establecido en la Sentencia T-280 de 2022, la expectativa de privacidad de los ciudadanos aumenta correlativamente en función de los espacios. En los lugares públicos hay expectativa de intimidad aun cuando esta sea baja. Pero tal expectativa aumenta cuando se trata de espacios semiprivados y privados:

Espacio

Expectativa razonable de intimidad

Privado

Máxima

Semiprivado

Alta

Semipúblico

Moderada

Público

Baja

12. El hecho de que la expectativa de privacidad en los espacios públicos sea baja no significa que el Estado o los particulares puedan instalar CCTV en cualquier espacio público, monitorear las actividades en esos escenarios o difundir lo que allí hacemos y ha quedado grabado. En eso, nuestra jurisprudencia sigue a otros tribunales del mundo. Por ejemplo, en la misma Sentencia T-280 de 2022, se ha reiterado uno de los precedentes más importantes del Tribunal Europeo de Derechos Humanos (en adelante TEDH) sobre estos dispositivos:

“(…) la videovigilancia de lugares públicos entra dentro del alcance del artículo 8 cuando los datos visuales se graban, se almacenan y se hacen públicos (Peck c. Reino Unido, §§ 57-63). En particular, proporcionar a los medios de comunicación, para su difusión, un vídeo del intento de suicidio de una persona captado por un circuito cerrado de televisión fue considerado como una injerencia grave en su vida privada, pese a encontrarse en un lugar público en el momento de los hechos”.

13. Reitero que si tenemos intimidad (o expectativa de intimidad) en el espacio público, con mayor razón esa expectativa aumenta en cuanto los espacios se hacen semiprivados o privados. Cuando estamos dentro espacios privados o semiprivados, como nuestros edificios o lugares de habitación que cuentan con CCTV, nuestra expectativa de intimidad es alta o máxima. Por eso, el TEDH ha limitado la instalación de CCTV en espacios semipúblicos o semiprivados:

“Además, en el asunto Antović y Mirković c. Montenegro, que se refería a la instalación de equipos de videovigilancia en aulas universitarias, el Tribunal señaló que la videovigilancia en el trabajo, sea secreta o no, constituye como tal una intrusión considerable en la “vida privada” del empleado”.

14. Dado que el ámbito de protección de nuestro derecho a la intimidad se amplía desde un contenido básico en el ámbito público hasta un contenido robusto en los lugares privados, considero que la finalidad de prevención de la medida objeto de control era, como se decidió, altamente inconstitucional. Esa finalidad era amplia, ambigua e indeterminada. Además, constituía una carta abierta para que la Policía accediera a los CCTV privados con fines generales, sin justa causa específica y sin apelar a otros medios menos lesivos de nuestras libertades.

3. Es necesario acotar el uso de los datos a los que se accede mediante la videovigilancia de los CCTV

15. En tercer lugar, creo que la limitación de la videovigilancia mediante los CCTV no solo debe recaer sobre la justificación para el acceso, sino que se debe extender a sus posibles usos. Se trata de evitar el desvío gradual de la función que suele ocurrir con este tipo de prácticas que confieren amplia consulta de datos personales. La disposición controlada en esta ocasión no prevé ningún mecanismo para evitar que, una vez obtenida la información, se desvíe el uso. De allí que fueran imprescindibles algunos parámetros para determinar lo que ocurre con el material al que la Policía tiene acceso y el control de búsquedas abusivas en los sistemas privados de CCTV.

16. En ese sentido, creo que se puede fijar una especie de regla de última ratio. Eso significa que el acceso a los circuitos privados de CCTV no es necesario ni legítimo cuando otros medios permiten la individualización o judicialización. Este criterio se aplica en Alemania para

la videovigilancia pública y creo que debe operar también -y con mayor razón- para obtener imágenes de los CCTV privados:

“La licitud de las videocámaras, según lo establecido en el § 6b BDSG, se hace depender de que la videovigilancia sea necesaria, es decir adecuada para lograr los objetivos fijados previamente y no exista otro medio igual de efectivo que pudiera limitar en menor medida el derecho a la autodeterminación informativa de los afectados por ella. Por tanto, el empleo de estos sistemas no será legítimo cuando puedan alcanzarse a través de otros instrumentos menos invasivos los mismos fines. La seguridad de un local en ocasiones se puede garantizar por otros medios sin tener que acudir a la grabación de imágenes, por ejemplo, reformándolo simplemente para mejorar su iluminación, o contratando a personal para que custodie sus accesos”.

17. De manera que no solo era necesario establecer las finalidades (bien precisas) que justificaban la medida sino el uso (también limitado) de esos datos o imágenes. Ello implicaba precisar la autoridad encargada de usar la información: un ser humano, una autoridad específica de policía o un algoritmo. Asimismo, era fundamental advertir que la videovigilancia es anónima (se desconoce a la persona que observa lo que la cámara capta) y por eso es más difícil atribuir responsabilidades. Por eso la ley debió indicar las finalidades legítimas y las autoridades que responderán por los malos usos de la información a la que se accede.

4. La relación con el derecho a la autodeterminación informativa

18. En cuarto lugar, me parece que hay elementos del derecho a la autodeterminación informativa que se deben implementar. Por ejemplo, el derecho a saber que las imágenes del CCTV podrían ser usadas directamente por la Policía o que están siendo usadas en una investigación. Quizá también el derecho a una mínima corrección. El derecho a indicar que no

se es la persona que aparece en el video y que podría haber sido, por ejemplo, testigo de una conducta.

19. Por eso creo que la ponencia debió analizar el siguiente aspecto de la relación entre la videovigilancia y la autodeterminación informativa. La regulación del Consejo de Europa sobre los principios directivos para la protección de las personas respecto a la recopilación y el tratamiento de datos a través de la videovigilancia (Resolución 1604/2008). En esta Resolución se han establecido limitaciones, cargas y responsabilidades asociadas al poder de videovigilancia de las autoridades. Además de prohibir el reconocimiento facial masivo, se indica que la videovigilancia debe ser objeto de:

“(…) una utilización pertinente, adecuada y no excesiva respecto a la finalidad que se persigue; evitar que los datos recopilados sean indexados, comparados y conservados sin necesidad; no efectuar una videovigilancia si el tratamiento de los mismos puede producir una discriminación contra algunos individuos o grupos de individuos, por razón de su opinión política, de sus convicciones religiosas, de su vida sexual, de sus características raciales o étnicas; informar claramente y de forma adecuada a las personas indicando la finalidad del sistema y la identidad de los responsables; garantizar el ejercicio del derecho de consultar sus imágenes y grabaciones; y por último, proteger la seguridad e integridad de todos los afectados a través de toda medida técnica y organizativa necesaria”.

20. Entonces no solo se trataba de limitar la finalidad y el uso de esa información recopilada sino de implementar todas las garantías compatibles del derecho a la autodeterminación informativa y la protección de datos personales. Por ejemplo, el deber de eliminación de la grabación a la que se ha accedido cuando esta ya no sea útil dentro de la investigación, la existencia de protocolos que limiten el número y la calidad de los espectadores de esos videos o imágenes o la delimitación de las imágenes necesarias para cada finalidad.

21. Permítanme un ejemplo: si he ingresado al edificio en el que se ubica mi residencia después de una cena con mi esposa y durante el ingreso nos hemos besado y alguna cámara ha captado ese momento. Y un par de minutos después, la misma cámara capta a una persona que ha sustraído un elemento de valor de alguna de las residencias. ¿Tiene sentido y legitimidad que el video al que acceden las autoridades incluya el momento previo en el que aparecíamos mi esposa y yo? ¿podemos solicitar que se elimine esa parte del video del material recaudado por la autoridad? Si luego ese video se difunde en los medios de comunicación -como ocurre diariamente en nuestros telediarios- ¿podemos solicitar que se deje de difundir esa parte del video? ¿cuál es el interés de esa parte del video para la Policía, un juez o la opinión pública?

22. Incluyo este ejemplo (de mi propia cosecha) porque impacta lo que ocurre diariamente con este tipo de información de los CCTV. Asistimos a la difusión masiva en las redes sociales y en los telediarios de las imágenes en directo de delitos sin la debida precaución por la protección de terceros (i.e. potenciales testigos), de niños y niñas o, inclusive, de los espectadores que asisten en vivo a imágenes de personas que disparan a otras en recintos vigilados mediante CCTV. De manera que el derecho a la autodeterminación informativa tiene un papel relevante que debió ser analizado por la Sala Plena bajo este enfoque.

5. La videovigilancia y su impacto individual y colectivo: el necesario principio de precaución

23. Por último, me interesa llamar la atención sobre el impacto en el comportamiento humano individual y social de la videovigilancia. La sola existencia de un diseño de la sociedad de la vigilancia modifica el comportamiento humano y restringe las libertades públicas. Se ha vuelto un lugar común señalar que la existencia del gran hermano (Orwell) o del panóptico ha dejado de ser una distopía. Si ello es así, a la Corte Constitucional le corresponde la máxima preservación de las libertades en el marco de una sociedad de la vigilancia. Comparto con uno de los supervisores adjuntos europeo de protección de datos que:

24. Si ello es así, entonces la Corte Constitucional se debió preguntar si era legítimo constitucionalmente que se construyera ese tipo de sociedad. Si cualquier avance digital o tecnológico debe estar al servicio de la seguridad y ser implementado en nombre de ese mismo propósito. Yo creo que la decisión de la Corte debió recuperar la libertad que aparece limitada con la sola existencia de los CCTV. Esa limitación aparece todavía más fuerte cuando se habilita a la Policía para acceder a lo que esos mecanismos recopilan.

25. Considero que también opera una suerte de principio de precaución. Este debe influir en el diseño de las medidas de videovigilancia e implica una serie de límites con el fin de proteger otros derechos (i.e. intimidad y autodeterminación informativa). Incluyo algunos ejemplos que adicionan lo que ya he comentado: i) la videovigilancia y el acceso a los CCTV solo se puede usar cuando sea estrictamente necesaria para lograr la finalidad taxativa que ha sido previamente prevista; ii) en “ningún caso puede la observación focalizarse en una persona concreta”; iii) solo se realiza en lugares públicos o semipúblicos (por ejemplo, las entradas y salidas de edificios residenciales se consideran espacios privados porque solo son usadas por los residentes y visitantes); iv) las limitaciones aplican para todos los dispositivos con capacidad para transformar la luz en una señal eléctrica (eso incluye webcams o cámaras incorporadas en teléfonos (iPhone)); v) se excluye la videovigilancia con fines comerciales, por hobby o afición y vi) se deben evitar las acciones de perfilamiento comercial o de otro tipo que no están directamente vinculadas a los fines de protección general que fundamentan la vigilancia.

26. Con base en todo lo anterior, creo que la Sala debió analizar si los puntos resolutivos eran suficientes para proteger todos los derechos, bienes y libertades que la habilitación objeto de control implicaba. Creo que los insumos que he puesto aquí ameritan otro tipo de condicionamientos tanto de parte motiva como de parte resolutive en el marco de la recuperación de las libertades que es, en buena medida, la esencia de la adjudicación

constitucional.

Fecha ut supra

JOSE FERNANDO REYES CUARTAS

Magistrado