COMENTARIOS A LOS SISTEMAS DE VIDEO VIGILANCIA EN EL MARCO DEL RÉGIMEN DE PROTECCIÓN DE DATOS PERSONALES

FEDERICO DELGADO AGUILAR

Monografía para optar al título de Abogado

Asesor: Luis Felipe González López

UNIVERSIDAD EAFIT

ESCUELA DE DERECHO

MEDELLÍN

2019

Introducción

Comenzar hablando de historia importa no porque pueda determinar o sustentar un fenómeno sino porque permite visibilizar el por qué llegamos hasta cierto punto; el carácter imbricado del asunto. En este caso en particular repasar la historia nos conducirá a reflexionar sobre el fenómeno de la videovigilancia y la incidencia de la normatividad de protección de datos personales sobre esta en Colombia. Hay una frase atribuida a Benjamin Franklin que dice "Aquellos que renuncien a la libertad esencial para adquirir un pedazo temporal de seguridad no merecen ni la libertad ni la seguridad."[1][2]. Esta frase resume de buen grado la posición que asume como insacrificable el valor de la vida privada, incluso a pesar de los posibles riesgos de seguridad y bienestar que implican tal decisión. No obstante también es cierto que las condiciones, la escala y los efectos de la violencia y del estilo de vida de las democracias modernas han cambiado drásticamente desde los tiempos de Franklin hasta la actualidad.

En ocasiones hay acontecimientos que funcionan como detonantes de cambios múltiples e impredecibles en diferentes esferas de la sociedad. Aun después de que ciertas condiciones iniciales pasen a un segundo plano sus efectos logran encausar políticas de gobierno y agendas legislativas, agitar debates o cambiar el discurso frente a una diversidad de otros asuntos particulares. En esta introducción hablaremos sobre la historia de dos asuntos que, si bien confluirán en algún momento, es importante aislarlas desde el principio. Estos son: i) el sometimiento de los ciudadanos a la vigilancia del Estado; y ii) la recolección y uso de información personal sobre los mismos. Las conversaciones alrededor de estos

[1] Todas las traducciones del inglés son propias a menos que se indique lo contrario.
[2] Benjamin Franklin, "Pennsylvania Assembly: Reply to the Governor, November 11, 1755", en *The Papers of Benjamin Franklin*, ed. Leonard W. Labaree, (Filadelfia: The Packard Humanities Institute, 1963), 242.

temas han tomado rumbos drásticos gracias a los efectos de varios sucesos particulares dados en el último siglo, hasta el punto de modificar y configurar un nuevo estado de cosas. Algunos acontecimientos puntuales son fáciles de determinar dado su grado de impacto y difusión. Otros se estructuran de forma más lenta y gradual, siendo realmente notorios en retrospectiva.

El uso de información personal de los ciudadanos fue una importante ayuda para los gobiernos que buscaban la violación sistemática de derechos humanos durante la primera mitad del siglo XX. Edwin Black relata como el Tercer Reich se valió de tecnología proveída por la filial de IBM en Alemania para identificar y clasificar a las víctimas del holocausto con tarjetas perforadas basándose en datos recogidos por censos: "La clave de los homosexuales era el número tres, a los judíos les correspondía el número ocho, a los 'antisociales' el nueve y a los gitanos el 12."[3] Y no solo fueron censos llevados a cabo por el Reich. Para 1942, en la Conferencia de Wannsee (aquella en la que se planeó la 'solución final' [*Endlösung der Judenfrage*]) los alemanes obtuvieron un registro con información detallada de los más de 1300 miembros de la comunidad judía en Noruega.[4] Más del cincuenta por ciento de los noruegos judíos fueron exterminados.[5] Situación similar a la que se dio en los Países Bajos donde a pesar del esfuerzo de la resistencia de incendiar todos los registros, los nazis también lograron identificar y deportar a miles de miembros de la comunidad judía.[6] En comparación con Dinamarca y Finlandia, donde el uno y menos del

[3] Edwin Black, *IBM y el holocausto: la alianza estratégica entre la Alemania nazi y la más poderosa corporación norteamericana* (Madrid: Editorial Atlántida S.A., 2001)
[4] Espen Søbye, *A dark chapter in the history of statistics?* (Oslo: Statistics Norway, 2006), acceso el 11 de noviembre del 2018, https://www.ssb.no/en/befolkning/artikler-og-publikasjoner/a-dark-chapter-in-the-history-of-statistics-1
[5] Ibíd.
[6] William Seltzer, "Population Statistics, the Holocaust, and the Nuremberg Trials", *Population and Development Review* 24, n° 3 (1998): 511-552.

uno por ciento fueron exterminados[7], es difícil distanciarse de la idea de cómo dichas estadísticas le facilitaron el trabajo al Reich. El uso discriminatorio de información confiada a los gobiernos no es exclusivo de regímenes tiránicos o de fuerzas de ocupación. Poco después del ataque a Pearl Harbor el gobierno de Franklin D. Roosevelt se ayudó de datos recogidos en los últimos censos realizados para ubicar y relocalizar a campos de concentración a 120.000 personas, muchos de ellos ciudadanos americanos con ascendencia nipona[8].

La combinación de grandes cantidades de información y tecnologías con capacidad de procesarla son instrumentos flexibles que incluso en manos de gobiernos legítimos y constitucionales tienen el potencial de causar graves daños. Estos y muchos otros casos en los que la información fue utilizada como una herramienta de control y opresión social (y hasta genocidio) impulsaron los debates para crear mecanismos legales que prevengan o reduzcan el riesgo de eventos similares. Por ejemplo, en Suecia se están discutiendo propuestas como la siguiente:

> Bajo amenaza de ocupación puede existir una causal para remover o destruir instalaciones de computación y los registros necesarios, esto en orden de prevenir que dicha información e instalaciones caigan en manos enemigas. Un enemigo podría, a modo de ejemplo, desear adquirir registros de población y otra clase de archivos que puedan ayudarle en su campaña de guerra. Pueden existir causales

[7] Søbye. *A dark chapter in.*
[8] Margo Anderson y William Seltzer, "Census Confidentiality under the Second War Powers Act (1942-1947)" en *Paper prepared for the Annual Meeting of the Population Association of America* (Nueva York: 2007) acceso el 17 de enero del 2019, http://margoanderson.org/govstat/integrity.htm

para revisar la manera en la cual se decidirá qué sistemas de procesamiento deberían ser destruidas o removidas en una situación de guerra.[9]

Por otro lado, la historia de la videovigilancia también se vio afectada por acontecimientos puntuales en tanto puntos de inflexión, abriendo las puertas la masificación de este fenómeno. Mark Hansen cree que en 1993 en Tacoma, Washington (EE.UU.) se instalaron las primeras cámaras operadas por la policía en espacio público en este país. Pero que fue Baltimore la que se recibió mayor atención como la ciudad vanguardista en la implementación de sistemas de videovigilancia en espacios públicos. En 1996, continúa el autor, se instaló un sistema que cubría un área de 16 cuadras. Este proyecto reportó una disminución del 11% en la criminalidad de este sector en el primer año y atrajo la atención de alguaciles de otras ciudades del país.[10] Las bombas del IRA y otros ataques terroristas pudieron ser decisivos para que el Reino Unido se volviese un referente de la vídeo-vigilancia. Varias estimaciones se han hecho sobre cuantas cámaras observan a los británicos. En 2013 un artículo publicado en *The Telegraph* estimaba que en el país habían entre 4.9 y 5.9 millones: una cámara por cada 11 o 14 habitantes.[11] Y no solo fueron estos ataques los que dispararon el uso de videocámaras. En 1993 fue asesinado, después de ser secuestrado y torturado, James Bugler, un niño de dos años.[12] Las imágenes capturadas por diferentes

[9] *Transnational Data Report* 1, no. 5 (1978), 17.
[10] Mark Hansen, "No Place to Hide: If crime is everywhere, so, too, may be police surveillance cameras and contraband detection devices to combat it. But who's looking out for privacy rights?" *ABA Journal* 83, n°8 (1997): 44-48, http://ezproxy.eafit.edu.co:2111/stable/27839966
[11] David Barret, "One surveillance camera for every 11 people in Britain, says CCTV survey", *The Telegraph,* 10 de julio del 2010, acceso el 17 de enero de 2019, https://www.telegraph.co.uk/technology/10172298/One-surveillance-camera-for-every-11-people-in-Britain-says-CCTV-survey.html
[12] "CCTV: Does it work?", *BBC News,* 13 de agosto del 2002, acceso el 24 de enero de 2019, http://news.bbc.co.uk/2/hi/uk_news/2071496.stm

cámaras fueron claves para la detención y juicio de Robert Thompson y Jon Venables, los dos niños de diez años responsables de la abducción y homicidio de Bugler.[13]

Con casos como el anterior pareciera que son ciertos acontecimientos traumáticos (ataques terroristas, asesinatos en serie) los que impulsan los cambios en las políticas criminales, de seguridad y en general del discurso público sobre la implementación de medidas preventivas. Estas medidas son cada vez más agresivas, acercándonos cada vez más rápido a las descripciones distópicas de la literatura. El caso Bugler, los atentados del 11 de septiembre de 2001 en Nueva York, los ataques del 11 de marzo de 2004 en Madrid y en Colombia el homicidio de Yuliana Samboní son ejemplos representativos de estos acontecimientos. Estos sucesos y discursos como el de la guerra contra el terrorismo, el de 'recuperar' zonas en ciudades o el de 'cuidar a nuestros niños' volvieron a la sociedad un ente pasivo, dócil y dispuesto a someterse a lo que Roger Clarke denomina 'datavigilancia' [dataveillance]: "el uso sistemático de información personal en la investigación o en el monitoreo de las acciones o comunicaciones de una o más personas".[14] Las deliberaciones sobre si se va a tolerar este fenómeno se llevaron a cabo en otros países. La mayoría se quedó esperando las 'telepantallas' de Orwell como el habilitador del totalitarismo mientras permitíamos formas muy superiores de vigilancia. Orwell tampoco previó que nuestro monitoreo también fuese hecho por privados muchas veces con intereses diferentes al de la seguridad. No escondieron las herramientas, nos las exhiben como una garantía de bienestar, como un servicio que luego se afianza como imperativo.

[13] Ibíd.

[14] "Information, Technology and Dataveillance", *Roger Clarke's 'IT and Dataveillance',* noviembre de 1987, acceso el 17 de enero del 2019, http://www.rogerclarke.com/DV/CACM88.html

En Colombia reina una política criminal reactiva y retributiva que ha encontrado elementos atractivos en los bajos costos de operación de sistemas de video-vigilancia, además de apostarle a las tecnologías emergentes que se valen de los datos personales. En el año 2015 el gobierno proyectaba adicionar para el año 2018 6.100 cámaras a las 4.564 instaladas entre los años 2011 y 2014 en todo el país.[15] Esto sin contar aquellas adquiridas por privados de las cuales no hay estimaciones.

Hansen[16] sostiene que tal vez aceptamos la invasión en nuestra vida privada y libertades personales porque reconocemos la necesidad de mayor seguridad en una sociedad violenta y porque consideramos que la molestia de ser monitoreados es justa a cambio de nuestra tranquilidad y bienestar. No obstante vivimos en un mundo en constante estado de crisis y pánico con formas de vigilancia masiva que permean todos los aspectos de nuestras vidas, nos convierten a todos en sospechosos y funcionan por el principio de drenar el pantano para atrapar cada serpiente[17]. Cuando la eficiencia es priorizada y las políticas se orientan en buscar individuos que encajen en un perfil predeterminado, se requiere por un lado muchísima precisión tecnológica y humana y por el otro un marco legal sólido. A pesar de la aparente apatía por la privacidad generalizada, en el área del Derecho se ha discutido y reconocido el riesgo que dichas tecnologías representan para diferentes derechos humanos fundamentales que con frecuencia son asociados, insistiendo en la necesidad de

[15] En 2018 habrá 10.664 videocámaras para fortalecer la seguridad ciudadana en el país, *Portal Web DNP*, 14 de junio del 2015, acceso el 17 de enero del 2019, https://www.dnp.gov.co/Paginas/En-2018-habr%C3%A1-10-664-videoc%C3%A1maras-para-fortalecer-la-seguridad-ciudadana-en-el-pa%C3%ADs.aspx

[16] Hansen, "No Place to Hide", 44-48.

[17] Ambrose Evans-Pritchard, "US asks Nato for help in 'draining the swamp of global terrorism", *The Telegraph,* 27 de septiembre del 2001, acceso el 17 de enero del 2019, *https*://www.telegraph.co.uk/news/worldnews/northamerica/usa/1357781/US-asks-Nato-for-help-in-draining-the-swamp-of-global-terrorism.html

salvaguardarlos. Estos son principalmente el derecho a la privacidad, a la intimidad, y el *habeas data* o autodeterminación informática.

Los dos primeros han sido ligados con el artículo 12 de La Declaración Universal de Derechos Humanos, el cual consagra que *"*Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques." El juez Thomas M. Cooley se refirió a la privacidad en los términos de "dejar en paz al otro [to be let alone]"[18]. Otras dimensiones de la privacidad por fuera de la del recogimiento como un derecho han sido desarrolladas en la jurisprudencia americana. La expectativa razonable de privacidad es un concepto utilizado por el juez John Marshall Harlan en su opinión concurrente en Katz v. United States, 389 U.S. 347 (1967). Este caso giraba en torno a la Cuarta Enmienda[19] y a las nuevas tecnologías para requisas policiales y vigilancia:

> Como la opinión de la Corte señala, "la Cuarta Enmienda protege a la gente, no a los lugares o establecimientos." La pregunta entonces es qué clase de protección se le brinda a la gente. Generalmente, como en este caso, la respuesta a esta pregunta requiere referirse a un "lugar", un establecimiento. Mi comprensión de la norma que ha surgido a partir de decisiones previas es que el requisito es doble: *primero, que haya una persona exhibiendo una expectativa actual (subjetiva) de*

[18] Thomas M. Cooley, "General Classification of Legal Rights", en *A Treatise on the Law of Torts or the Wrongs Which Arise Independent of Contract*, (Chicago: Callaghan, 1879), 29.

[19] "Enmienda IV. El derecho del pueblo a la seguridad que sus personas, domicilios, papeles y efectos se hallen a salvo de pesquisas y aprehensiones arbitrarias, será inviolable, y no se expedirán órdenes, excepto con motivo probable, sustentados mediante juramento o promesa, y expresamente describiendo el lugar que será registrado y las personas o cosas que han de ser detenidas o incautadas."

> *privacidad y, segundo, que dicha expectativa sea una tal que la sociedad esté dispuesta a aceptar como "razonable".* Por lo tanto el hogar de un hombre es, para la mayoría de casos, un lugar donde él puede esperar privacidad, pero los objetos, actividades o afirmaciones que él exponga a "plena vista" de desconocidos no están "protegidos" porque no hay ninguna intención exhibida de que él prefiera quedarse estas cosas para sí mismo únicamente. Por otro lado, las conversaciones en el mundo abierto no serán protegidas contra la escucha casual o inintencionada, pues la expectativa de privacidad bajo tales circunstancias no sería una expectativa razonable. [Itálicas nuestras]

La expectativa no limita la privacidad como siendo únicamente el derecho a estar solo; la presenta también como parte de la libertad de locomoción. En este sentido la expectativa razonable de privacidad consiste en que si bien uno debe ser consciente de la relativa poca privacidad que existe cuando se está en público, de ahí no se sigue que debamos esperar ser vigilados por alguien a kilómetros de distancia y por largas duraciones de tiempo. El derecho a la privacidad vista hasta ahora es una condición humana. Tanto como expectativa de no estar siendo observado como en tanto la posibilidad de estar solo. Este doble criterio puede servir como base de entrada para analizar la viabilidad del despliegue de sistemas de vigilancia masivos.

Con el desarrollo tecnológico y el poder informático llegaron transformaciones para la relación del ser humano con su entorno haciendo necesario el reconocimiento de nuevos derechos. El *Big Data*, la nube y la analítica de datos son temas cada vez más populares, y

como en el caso de Cambridge Analytica[20] y los diferentes *leaks*, su uso indebido ha protagonizado grandes escándalos. Los datos personales han sido denominados en incontables entrevistas y publicaciones como el nuevo petróleo o una nueva moneda. El Derecho no podía permanecer inmóvil ante la amenaza del flujo y uso indiscriminado de los datos. Es así como el derecho a la autodeterminación es una respuesta a las prácticas tanto en los sectores públicos y privados de recolectar, procesar y almacenar datos personales para todo tipo de fines. Entre ellos la seguridad y vigilancia. Con ponencia del magistrado Ciro Angarita Barón, en sentencia T-414 de 1992 la Corte Constitucional introduce a la jurisprudencia esta idea:

> La posibilidad de acumular informaciones en cantidad ilimitada, de confrontarlas y agregarlas entre sí, de hacerle un seguimiento en una memoria indefectible, de objetivarlas y transmitirlas como mercancía en forma de cintas, rollos o discos magnéticos, por ejemplo, permite un nuevo poder de dominio social sobre el individuo, el denominado poder informático.[21]

Y como respuesta o contrapeso, "este nuevo poder ha engendrado la libertad informática. Consiste ella en la facultad de disponer de la información, de preservar la propia identidad informática, es decir, de permitir, controlar o rectificar los datos concernientes a la personalidad del titular de los mismos y que, como tales, lo identifican e individualizan ante los demás."[22]

---

[20] Carole Cadwalldr, "'I made Steve Bannon's psychological warfare tool': meet the data war whistleblower", *The Guardian*, 18 de marzo del 2018, acceso el 26 de noviembre del 2018, https://www.theguardian.com/news/2018/mar/17/data-war-whistleblower-christopher-wylie-faceook-nix-bannon-trump

[21] Corte Constitucional, STC C-748 de 2011, numeral 2.5.6. Magistrado Ponente Ciro Angarita Barón.

[22] Ibíd.

En otras palabras, la autodeterminación informática se puede definir como el derecho de un individuo a tener control sobre el conocimiento y la difusión de sus datos personales. La autodeterminación informática o *habeas data* "otorga facultades al titular de los datos personales para que este decida las circunstancias de lugar, tiempo y modo en que ha de recabarse y tratarse su información personal."[23] Este derecho es de carácter personalísimo e independiente de otros como la privacidad, la intimidad y el honor, aunque son asociados con frecuencia. Entonces una noción de privacidad informática tendría hasta ahora dos componentes principales: la privacidad que como se ha dicho, es una condición humana. El segundo componente es el control sobre la información; los terceros que tienen acceso a ella, los fines para los que es usada y el nivel de difusión. La importancia que se le dio a estos temas a partir de 1970 resultó que en el año 2000 la Unión Europea incorporara en su Carta de los Derechos Fundamentales (2000/C-364/01) el derecho a la protección de datos de carácter personal:

> Artículo 8. 1. Toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan. 2. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a su rectificación.3. El respeto de estas normas quedará sujeto al control de una autoridad independiente.

[23] Omar Mendoza, "El derecho a la autodeterminación informativa en la era de la llamada videovigilancia en el sector privado en México. Una perspectiva desde la Ley Federal de Protección de Datos Personales en Posesión de Particulares y los retos pendientes", en *Revista de Derecho, Comunicaciones y Nuevas Tecnologías*, n° 12 (2014): 8.

A pesar de estos logros el *habeas data* y el derecho a la protección de datos personales no ha tenido una respuesta legislativa uniforme en todo el mundo. Predominan dos modelos o enfoques que han adoptado los ordenamientos jurídicos: el de la protección a la privacidad y el de la protección de datos personales.

La visión norteamericana favorece un modelo que entiende la privacidad del individuo como un bien disponible y la protección de datos como un derecho del consumidor. Los titulares cuentan con mecanismos que les dan voz y control sobre sus datos y este decide si prefiere mantenerlos privados o explotarlos como un bien negociable. Los Estados Unidos plantean un sistema de varias normas sectoriales y autorregulación sin la necesidad de una entidad gubernamental que las apoye.[24]

Lloyd[25] expone que el manejo que le ha dado Europa a la protección de datos es burocrático y paternalista, y abarca todos los aspectos del procesamiento de datos personales teniendo presente la protección de datos como un derecho fundamental. Los europeos crearon agencias que están alerta y listas ejerciendo funciones de vigilancia, control y sancionatorias para entrar a proteger los intereses de un individuo o de la comunidad. El establecimiento de autoridades independientes de control es una garantía para la adecuada implementación de las normas de protección de datos. En el modelo europeo el *good will* de la autorregulación no basta y saben que muchas personas no cuentan con el tiempo ni los recursos para poner en marcha los mecanismos que propone un diseño que pone al individuo en el centro. Si bien una institución está mejor posicionada para vigilar estas actividades, estas pueden verse obstaculizadas por los trámites legales y en cierta medida los intereses del Estado que podrían

[24] Nelson Angarita, *Tratamiento de datos personales: aproximación internacional y comentarios a la ley 1581 de 2012,* (Bogotá: Legis Editores S.A., 2013).
[25] Ian J. Lloyd, *Information Technology Law,* (Oxford, Oxford University Press, 2011)

llegar a colisionar con los de la privacidad de la población. Sin embargo parece que el modelo europeo logró volverse el estándar internacional debido en gran parte a lo que se conoce como el 'nivel adecuado de protección'. El artículo 29 de la Directiva 95/46/CE creó El Grupo de Protección de las Personas en lo que Respecta al Tratamiento de Datos Personales. Entre 1997 y 1998 el Grupo produjo varios documentos[26] que discutían el nivel de protección de datos existente dentro de la Unión y en países terceros para así establecer reglas para la transferencia de datos entre unos y otros. En ellos se estudiaban los derechos en cabeza del titular de los datos, los mecanismos y procedimientos con los que cuenta para hacerlos valer, las obligaciones de los que realizan el tratamiento y la existencia de una autoridad independiente que controle, vigile, sancione y reciba las quejas de los ciudadanos. Se fue construyendo entonces el contenido mínimo de las regulaciones de terceros países basándose en los estándares y principios plasmados en la Directiva y otros documentos internacionales[27]. Estudiados los informes, la Comisión Europea dictamina a qué países les otorga un nivel adecuado de protección para la transferencia de datos personales. Hoy en día los Estados miembros de la Unión Europea han suscrito compromisos posteriores por los cuales buscan impedir que durante la exportación de datos personales a países o territorios que no posean un nivel adecuado de protección de datos (referidos con frecuencia como *data havens*) disminuya el nivel de protección que se le garantiza al Titular dentro de la Unión.

La disparidad entre el modelo europeo y el americano ha presentado problemas dada la estrecha relación comercial y por ende el alto flujo de transmisión de datos entre los

[26] En el transcurso de estos dos años, el Grupo del artículo 29 publicó tres reportes anuales que cubrían el desarrollo de la protección de datos personales dentro y fuera de la comunidad. Acceso el 10 de enero de 2019, https://ec.europa.eu/justice/article-29/documentation/annual-report/index_en.htm

[27] Entre ellos las Directrices de la OECD de 1980, los principios establecidos en la resolución 45/95 de la Asamblea General de la ONU en 1990 y en el Convenio 108 de 1981 del Consejo de Europa.

Estados Unidos y los Estados miembros de la Unión Europea. Ambos llegaron a unos arreglos en el año 2000 que permitieron por muchos años que la Unión declarara que los EE.UU. ostentaban un nivel adecuado de protección de datos personales[28]. Sin embargo en el año 2015 el Tribunal de Justicia de la Unión Europea invalidó dicho acuerdo debido a los escándalos de espionaje masivo valiéndose de redes sociales como Facebook por la Agencia Nacional de Seguridad de Estados Unidos (la NSA por sus siglas en inglés).[29] Esto llevó a que en el 2016 ambas partes firmaran el EU-US Privacy Shield, un acuerdo político que fortaleciera las fallas del acuerdo anterior[30]. No obstante es probable que este fracase o sea una medida provisional. Activistas de la privacidad en Europa no creen que haya voluntad política por parte de los americanos.[31] Fuera de esto grandes compañías multinacionales cuyo activo principal son los datos como Google y Amazon han pedido al Congreso de EE.UU. que adopte un régimen general de protección de datos personales que los acerque al nivel de los estándares europeos[32]. Para dichas compañías lo anterior les evitaría problemas a la hora de almacenar y operar datos en EE.UU. que vienen de la Unión Europea y de otros países

[28] En la llamada "Safe-Harbour Decision" la Comisión Europea mediante Decisión 2000/520/CE del 26 de julio estimó que los Principios de puerto seguro para la protección de la vida privada en conjunto con la orientación que dan las preguntas más frecuentes (FAQ), publicadas por el Departamento de Comercio de Estados Unidos, garantizan un nivel adecuado de protección de datos personales para la transferencia de datos entre la Unión y los EE.UU.

[29] Comunicado de prensa de la Corte de Justicia de la Unión Europea, 6 de octubre del 2015, acceso el 17 de enero del 2019, https://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117en.pdf

[30] Comunicado de prensa de la Comisión Europea, 2 de febrero del 2016, acceso el 2 de diciembre del 2018, http://europa.eu/rapid/press-release_IP-16-216_en.htm

[31] The Economist Explains, "The new transatlantic data "Privacy Shield"", *The Economist*, 2 de febrero del 2016, acceso el 2 de diciembre del 2018, https://www.economist.com/the-economist-explains/2016/02/02/the-new-transatlantic-data-privacy-shield

[32] Dan Tynan, "Silicon Valley finally pushes for data privacy laws at Senate hearing", *The Guardian*, 27 de septiembre del 2018, acceso el 2 de diciembre del 2018, https://www.theguardian.com/technology/2018/sep/26/silicon-valley-senate-commerce-committee-data-privacy-regulation.

con niveles adecuados de protección. Todo indica que el modelo europeo prevalecerá por encima del americano al menos en occidente.

Siguiendo esta tendencia, en Colombia se promulgó Ley Estatutaria 1581 de 2012[33] la cual comenzó a darle forma al actual régimen de protección de datos personales (RGPDP). Si bien es la primera ley sobre disposiciones generales para la protección de datos personales, no es la primera normatividad sobre la materia en el país. El artículo 15 de la Constitución dispuso que:

> Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. *De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas.* En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución. [Itálicas nuestras]

La Constitución concibe al *habeas data* como un derecho fundamental autónomo[34]. También como un mecanismo de protección o herramienta constitucional para tener control sobre el tratamiento de sus datos personales y garantizar la protección de otros derechos fundamentales conexos.[35] Pasaron diecisiete años de desarrollo exclusivamente constitucional para que se promulgara la primera ley sobre protección de datos. Esta fue la Ley Estatutaria 1266 de 2008, "por la cual se dictan las disposiciones generales del hábeas

[33] *"por la cual se dictan disposiciones generales para la protección de datos personales."*
[34] "Es, además, un derecho fundamental autónomo que busca equilibrar las condiciones entre el sujeto de quien se informa y aquel que tiene la capacidad de recolectarlo, almacenarlo, usarlo, y transmitirlo." Ver sentencias T-307 de 1999 y T-1085 de 2001 de la Corte Constitucional, entre otras.
[35] Ver Sentencias T-110 de 1993, T-303 de 1998, T-321 de 2000, T-310 de 2003, entre otras.

data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones." Como su encabezado lo indica, esta ley es de carácter sectorial. Sin embargo recoge una serie de conceptos definidos[36] y principios[37] en su mayoría aplicables a todo tratamiento de datos. Finalmente fue promulgada la Ley 1581 de 2012. Cabe resaltar como la protección de datos personales en el ordenamiento colombiano tuvo su origen en el ámbito constitucional, seguido del sectorial y solo después en el general.

El ordenamiento jurídico colombiano no ha logrado evolucionar al ritmo que los avances tecnológicos exigen, dejando con frecuencia derechos fundamentales expuestos a abusos de todo tipo mientras la Ley reacciona y se adapta. El uso masivo de sistemas de videovigilancia justificado por la inseguridad en las ciudades sin ningún control o regulación sobre su implementación es un caso de lo anterior. Instaladas de forma indiscriminada, estas videocámaras una vez exclusivas de bancos y joyerías, ahora llenan todos los espacios por los que nos movemos cotidianamente. No solo es lo incomodo que es sentirse observado en lugares donde anteriormente se podía esperar algo de privacidad. La intimidad es limitada a contados lugares, se puede estar sujeto a arbitrariedades por parte de quienes están monitoreando estos sistemas y las imágenes recogidas pueden ser usadas para fines diferentes a la seguridad. Por otra parte, los costos de almacenamiento de datos al pasar de las cintas magnéticas a la nube ha bajado drásticamente y se han desarrollado herramientas de análisis de información al servicio de la industria de la seguridad. Todo sin la posibilidad de ejercer nuestro derecho a la autodeterminación informática y con pocos o ningún control de

[36] Artículo 3º de la Ley 1266 de 2008.
[37] Artículo 4º de la Ley 1266 de 2008.

autoridad alguna. Si bien el RGPDP intenta ser la respuesta a estos fenómenos, este posee algunos problemas. El régimen es inconstante al definir las bases de datos como un elemento relevante para su ámbito de aplicación y las obligaciones que impone. Asimismo se queda corto al momento de establecer parámetros que condicionen la instalación de sistemas de videovigilancia. La idoneidad del régimen también levanta sospechas al estudiar otros conceptos como el de datos sensibles y el consentimiento en el contexto de dichos sistemas. La raíz de las ideas expuestas reside principalmente en la lectura del régimen en función de elementos 'técnicos' propios de las tecnologías de la información y la videovigilancia. Si bien en un primer momento parecerán detalles menores, los efectos de estos serán muy preocupantes a medida que escalan los avances tecnológicos y se afianza la videovigilancia a la política de seguridad estatal y privada. Con esto se corre el riesgo de que el RGPDP quede rezagado y no pueda tutelar los derechos por los cuales fue concebido. El presente trabajo se abordará en un orden similar al de los problemas presentados. Sin embargo se empezará hablando de los principios del tratamiento de datos personales y su desarrollo dada su importancia como estructura orgánica de todo el RGPDP.

El principio de interpretación para el tratamiento de datos personales en los sistemas de video-vigilancia

La Corte Constitucional ha cumplido un papel fundamental en la fijación de principios relativos al tratamiento de datos personales. Esta contextualización ayudará a explicar cómo la aplicación de los principios que debe seguir el tratamiento adecuado de datos personales se aleja de la lógica implementada para interpretar el ámbito de aplicación de la Ley 1581 de 2012.

El contenido y el alcance de los derechos fundamentales amparados en el RGPDP, han sido desarrollados por la Corte Constitucional en ejercicio de sus funciones como intérprete de la Constitución. Desde sus inicios, la Corte había denunciado en repetidas ocasiones la ausencia de una ley estatutaria que regulara la protección de datos personales y la inexistencia de mecanismos ordinarios que ampararan los derechos relacionados con la manipulación de la información personal.[38] Así mismo, la Corte señaló en varias oportunidades que si bien la acción de tutela es importante a la hora de proteger los derechos al *habeas data* y la intimidad, la misma no constituía una herramienta suficiente y que no se trata únicamente de tener garantías *ex post* sino también de fijar reglas claras previas. En este sentido, la Corte invitó múltiples veces al Congreso de la República para que impulsara un proyecto de ley amplio e integral sobre la materia.

Así fue como, de cara al vacío normativo, a la aparición de nuevas tecnologías y a la necesidad en la sociedad de recolectar mayores cantidades de información, la Corte fue

[38] Ver sentencias T-414 de 1992, SU-082 de 1995, T-307 de 1999, T-729 de 2002, entre otras.

recogiendo una serie de principios y garantías[39] como una primera línea de defensa al *habeas data*, la autodeterminación informativa, el buen nombre y a la intimidad. Durante años la Corte fue la vanguardia en la protección de los derechos predicables del tratamiento de datos personales.

Todo esto hizo posible que hoy, de conformidad con el principio de interpretación[40] y la jurisprudencia que la Corte venía desarrollando sobre el tratamiento de datos, la totalidad del RGPDP deba interpretarse de forma tal que sea compatible con la Constitución y la jurisprudencia constitucional en la materia. Lo anterior fue también plasmado de manera puntual en el literal e) del artículo 4° de la Ley 1266 de 2008 en la forma del principio de interpretación integral de derechos constitucionales[41].

[39] Los principios de necesidad, finalidad, veracidad o calidad, integridad, incorporación, utilidad, circulación restringida, caducidad e individualidad se encuentran sistematizados en la sentencia T-729 de 2002. El desarrollo de los mismos se puede evidenciar en sentencias anteriores como las T-097/95, SU-082/95 y SU-089/95.

[40] La Corte Constitucional, en la sentencia C-1026 de 2001, definió el principio de interpretación como aquel "según el cual todos los mandatos del ordenamiento jurídico se deben interpretar de forma tal que su sentido guarde coherencia con las disposiciones constitucionales. Ello implica varias cosas: primero, que toda interpretación que no sea conforme a la Constitución, debe ser descartada; segundo, que ante dos interpretaciones posibles de una norma, el juez se debe inclinar por aquella que, en forma manifiesta, resulte más adecuada a los mandatos superiores; tercero, que en caso de dos o más interpretaciones que sean, en principio, igualmente constitucionales, el juez, en autonomía funcional, deberá escoger en forma razonada aquella que considere mejor satisface los dictados del constituyente en el caso concreto." Así mismo, en la sentencia C-539 de 2011, la Corte se refiere al alcance de sus providencias en los siguientes términos: "En suma, en relación con la obligatoriedad y alcance de la doctrina constitucional, la jurisprudencia de esta Corte ha aclarado que esta deviene de que la Constitución es norma de normas, y el precedente constitucional sentado por la Corte Constitucional como guardiana de la supremacía de la Carta tiene fuerza vinculante no sólo para la interpretación de la Constitución, sino también para la interpretación de las leyes que obviamente debe hacerse de conformidad con la Carta"

[41] "Principio de interpretación integral de derechos constitucionales. La presente ley se interpretará en el sentido de que se amparen adecuadamente los derechos constitucionales, como son el *hábeas data*, el derecho al buen nombre, el derecho a la honra, el derecho a la intimidad y el derecho a la información. Los derechos de los titulares se interpretarán en armonía y en un plano de equilibrio con el derecho a la información previsto en el artículo 20 de la Constitución y con los demás derechos constitucionales aplicables."

Lo anterior es importante porque, en primer lugar, en cierto sentido le impone una orientación o límites restrictivos que la LEPD le da su ámbito de aplicación, por lo menos, de los principios. La Corte Constitucional suele pronunciarse en términos de derechos. Su preocupación es que el derecho fundamental al *habeas data* y los demás conexos no sean vulnerados o violados. Con este fin en mente fue que erigió un sistema de principios y garantías que deban respetarse incluso en los casos exceptuados al régimen de aplicación de la Ley 1581[42], puesto que el tratamiento de datos personales es por sí solo suficiente para representar una posible amenaza a dichos derechos. Lo anterior teniendo en consideración los casos excepcionales en los que se puede presentar una tensión entre estos derechos y otros principios constitucionales o bienes jurídicos de especial importancia. En estas eventualidades se procederían a hacer los análisis necesarios[43]. La Corte interpretó que la finalidad de la LEPD apunta en la dirección de un régimen general para la protección de la información personal[44]. En el mismo sentido, el informe de ponencia para el segundo debate

[42] El tercer inciso del artículo 2° de la Ley 1581 establece que "la presente ley no será de aplicación: a) A las bases de datos o archivos mantenidos en un ámbito exclusivamente personal o doméstico (…); b) A las bases de datos y archivos que tengan por finalidad la seguridad y defensa nacional (…); 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; y f) A las bases de datos y archivos regulados por la Ley 79 de 1993." Sobre dicho inciso la Corte Constitucional se pronunció en la sentencia C-748 de 2011 diciendo que "estas hipótesis no están exceptuadas de los principios, como garantías mínimas de protección del habeas data. (…) son casos exceptuados –no excluidos- de aplicación a las disposiciones de la ley (…) salvo respecto de las disposiciones que tienen que ver con los principios."

[43] Sobre esto Rodrigo Uprimny y Diana Guarnizo se remiten a Robert Alexy y su noción de principios repetida en todas las facultades de Derecho de Colombia de generación en generación: "(…) la concepción de Robert Alexy, para quien los principios son normas que ordenan que se realice algo en la mayor medida posible de acuerdo con las posibilidades jurídicas y fácticas, de manera que operan como mandatos de optimización que pueden ser cumplidos en diversas formas y en diversos grados." Más adelante agregan: "(…) las tensiones entre diferentes principios deben ser resueltas a través de la ponderación." [Diana Guarnizo y Rodrigo Uprimmy, "¿Es posible una dogmática sobre la prohibición de regresividad?, *DeJusticia,* (2006), 20]

[44] Sentencia C-748/11: "[…] desde el punto de vista teleológico, estos preceptos deben interpretarse dentro del propósito del proyecto de ley: introducir en el ordenamiento una serie de principios básicos aplicables al tratamiento de todos los datos personales […]"

en el Senado para la aprobación de la Ley 1581 de 2012, evidencia que el legislador tenía la misma idea en mente al sostener que:

> […] sin importar la finalidad que tenga la base de datos, mientras contenga información y datos personales se deberá respetar los principios generales que regulan el tratamiento y la protección de datos; así lo ha sostenido en reiteradas ocasiones la Corte Constitucional al enunciar el desarrollo y alcance que deben tener los principios que regulan el tema de la protección de la información.

La consecuencia que se desprende de la sistematización de dichos principios sobre los sistemas de videovigilancia es que, de concluirse que en su operación se tratan datos personales, los mismos quedarán supeditados a aquellos. Es la sola captura de datos personales por las cámaras lo que sujeta las actividades de videovigilancia a los principios y garantías. E independientemente de cómo se les denomine, se les defina, o se les ubique en una pirámide, los principios y garantías terminan siendo preceptos normativos que a la larga imponen deberes y su desacato trae sanciones.

Ámbito de aplicación del RGPDP

El impacto y la importancia de la LEPD no se deben al reconocimiento de derechos individuales y libertades. La Asamblea Nacional Constituyente de 1991 analizó y promulgó disposiciones que le confieren protección constitucional a los derechos y libertades de los colombianos cuando su información personal es sometida a cualquier actividad de tratamiento. Posteriormente la Corte Constitucional y leyes como la Ley 1266 de 2008[45], introdujeron conceptos más especializados y propios del *habeas data* y la autodeterminación informática[46], y recogieron los principios necesarios para el desarrollo de la ley[47]. La LEPD no introduce la protección de información personal al ordenamiento jurídico colombiano, lo que trae es un sistema de protección con herramientas, mecanismos e instituciones que tutelan derechos, libertades y deberes. La ley asumiendo una postura garantista admite que no es posible hacer valer un derecho sin la correspondencia de un mecanismo jurídico que lo tutele y otorga vías legales a los titulares de los datos personales. Así es como se puede afirmar que el triunfo más importante fue entender que se requiere de transparencia y mecanismos verificables para que sea efectiva la implementación de una regulación al tratamiento de la información personal.

El inicio de la LEPD abre camino para pensar si videovigilancia es una actividad sujeta a este régimen y en qué grado. El artículo 2° dicta que "Los principios y disposiciones contenidas en la presente ley serán aplicables a los datos personales registrados en cualquier

[45] Que de acuerdo a su objeto, sus disposiciones están orientadas particularmente "en relación con la información financiera y crediticia, comercial, de servicios, y la proveniente de terceros países."
[46] El artículo 3° proporciona, entre otros, los conceptos de titular de la información, dato personal, dato público, dato semiprivado, dato privado.
[47] Los principios definidos por el artículo 4° de la ley son: (i) principio de finalidad; (ii) principio de libertad; (iii) principio de veracidad o de calidad; (iv) principio de transparencia; (v) principio de acceso y circulación restringida; (vi) principio de seguridad; (vii) principio de confidencialidad.

base de datos que los haga susceptibles de tratamiento por entidades de naturaleza pública o privada." Este aparte se puede fragmentar en tres condiciones: La primera es la existencia de datos personales. La segunda es que los datos deben estar registrados en una base de datos que los haga susceptibles de actividades de tratamiento. La tercera es que el tratamiento sea realizado por entidades de naturaleza pública o privada. Este fraccionamiento, la definición de algunos conceptos y el uso de casos de estudio, serán la estructura sobre la cual se hará gran parte del análisis acerca de la aplicación del RGPDP a la operación de sistemas de videovigilancia.

El dato personal es información sobre las personas. Cualquier referencia que me apunte o pueda llegar a apuntar a alguien más. De ellos se han realizado diferentes clasificaciones con miras a establecer los niveles de seguridad o las medidas que se deben tomar para garantizar al titular de la información un tratamiento lícito y responsable, algunas de las cuales serán abordadas en otro momento. Independientemente del tipo de información, si está por sí sola o en conjunto con otros datos, si revela aspectos sobre una persona identificada o identificable, su tratamiento debe someterse de manera integral a los principios para el tratamiento de datos personales. La Ley 1581 de 2012 entiende por dato personal: "Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables." La definición concuerda en términos generales con la desarrollada por la jurisprudencia Constitucional[48] en esta materia y con la establecida en la Ley 1266 de 2008. En este sentido, la Corte señaló en que el legislador podía adoptar una

[48] La primera aproximación jurisprudencial al concepto se encuentra en la sentencia T-414 de 1992, en la cual la Corte definió que se entiende por dato personal: "El dato que constituye un elemento de la identidad de la persona, que en conjunto con otros datos sirve para identificarla a ella y solo a ella […]" En la sentencia T-022 de 1993, la Corte afirmó: "Por su manifiesta incidencia en la efectiva identificación o posibilidad de identificar a las personas, tal característica le confiere al dato una singular aptitud para afectar la intimidad de su titular mediante investigaciones o divulgaciones abusivas o indebidas."

definición de dato personal en ejercicio legítimo de su libertad de configuración y que en el caso de la encontrada en la Ley 1581, no estaba desconociendo sus límites[49]. Esta definición se acerca más a la encontrada en diversos documentos internacionales[50], lo cual no resulta extraño teniendo en mente que una de las razones por las cuales el gobierno impulsó esta ley fue para alcanzar los estándares internacionales en materia de protección de datos personales.[51]

Considerando las definiciones presentadas, predicar la existencia de datos personales en la operación de los sistemas de videovigilancia privados como uno de los tres presupuestos o condiciones identificadas en el artículo 2° de la LEPD es indiscutible. Las cámaras, videocámaras como un circuito de televisión cerrada (CCTV por sus siglas en inglés) o las cámaras IP, entre otros medios que registran imágenes, capturan todo tipo de información personal sobre las personas que circulan por las áreas vigiladas como el rostro o las placas de sus vehículos. La sola transmisión en directo, sin ningún tipo de almacenamiento para su posterior consulta, debería hacerse con observancia de unas garantías y principios mínimos

[49] Corte Constitucional, STC C-748 de 2011, numeral 2.5.6.

[50] "Por datos personales se entenderá toda información correspondiente a una persona identificada o identificable (el sujeto de los datos)" [Literal b, numeral 1°, Directrices de la OECD de 1980]. "[T]oda información sobre una persona física identificada o identificable […] se considerará identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un número de identificación o uno o varios elementos específicos, característicos de su identidad física, fisiológica, psíquica, económica, cultura o social" [Literal a, artículo 2°, Directiva 95/46/CE]. "Cualquier información concerniente a una persona física identificada o identificable." [Numeral 5, artículo 3°, Ley Federal de Protección de Datos Personales en Posesión de los Particulares]. "[D]atos personales: toda información sobre una persona física identificada o identificable (<el interesado>): se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona" [Numeral 1, Artículo 4 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo].

[51] "[…] precisamente lo que se pretende con el proyecto en estudio, además de lograr una protección del dato personal en los términos en que lo exige la Constitución, es lograr que el país cumpla con los estándares internacionales en la materia para lograr las certificaciones necesarias para insertarse en el mercado, como un territorio con niveles adecuados de protección de los datos personales" [Corte Constitucional, STC C-748 de 2011, numeral 2.18.3.1.]

propios del debido tratamiento de datos personales toda vez que su finalidad puede desviarse de ser una simple herramienta de disuasión (seguridad) y volverse en una de discriminación y segregación social. Un caso ejemplar de un indebido tratamiento de información personal sin la necesidad de almacenamiento se dio en el centro comercial de Reforma 222, un complejo de edificios en el sector financiero de Ciudad de México[52]. En los días posteriores a la inauguración de la edificación, las cámaras de vigilancia empezaron a ser utilizadas para monitorear y detectar a miembros de la comunidad LGTBI que desplegaran formas públicas de afecto, como besos o abrazos. Una vez identificados, el personal de seguridad se les acercaba a pedirles que se comportaran de otra manera y de rehusarse, se les invitaba a irse del lugar[53].

Estudiada la condición de la existencia de datos personales, el artículo objeto de análisis además establece que dichos datos deben estar "registrados en cualquier base de datos que los haga susceptibles de tratamiento […]". Este fragmento del artículo 2° se vale de varios conceptos claves como el de base de datos, y al igual que el de datos personales, no es introducido al ordenamiento jurídico colombiano por la LEPD pero el legislador igualmente lo define en el literal b) del artículo 3° como un "conjunto organizado de datos personales que sea objeto de tratamiento". La Corte es acertada al calificar esta definición adoptada en la ley como "bastante amplia"[54] y más adelante dice que se ajusta a la Constitución porque "cobija todo espacio donde se haga alguna forma de tratamiento del dato, desde su simple recolección, lo que permite extender la protección del habeas data a

[52] Nelson Botello, "Regulación de la videovigilancia en México. Gestión de la ciudadanía y acceso a la ciudad", en *Espiral* 23, n°66 (2016), acceso el 17 de enero de 2019, http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S1665-05652016000200193
[53] Ibíd.
[54] Ver numeral 2.5.5. de la C-748 de 2011.

todo tipo de hipótesis."[55] Esta última interpretación de la Corte desconoce lo dicho por el legislador cuando de forma deliberada recurrió al término 'organizado' como un condicionante para el conjunto de datos personales que constituye una base de datos. Sin embargo, en la misma sentencia[56], la Corte provee diferentes definiciones de lo que el ordenamiento jurídico colombiano ha entendido por archivos, confiriéndoles siempre la característica de ser organizados y más adelante concluye que estos son "una especie de bases de datos"[57]. Si la Corte le confiere esta misma característica a las bases de datos no queda del todo claro, y será un asunto determinante más adelante. Pero el legislador, enmarcándose en las definiciones encontradas en ordenamientos extranjeros[58] y desde una perspectiva teleológica vio el uso de dicho término como algo imprescindible para que la LEPD se ajuste a los estándares internacionales de la protección de datos personales.

Analizando la definición proporcionada por el artículo 3° de la Ley 1581 de manera conjunta con la encontrada en diferentes documentos internacionales, se puede inferir que cuando el artículo 2° manifiesta que la ley aplica "a los datos personales registrados en cualquier base de datos *que los haga susceptibles de tratamiento* […]" [Itálicas nuestras] es esa accesibilidad a la información personal en función de diferentes criterios de búsqueda lo que la vuelve susceptible de actividades de tratamiento. En la medida en que el conjunto de datos personales posea una estructura como la descrita, se podrá decir que está organizado y conforma, para efectos de la LEPD, una base de datos. Este punto será retomado más adelante

[55] Ibíd.
[56] Ibíd., numeral 2.4.3.2.
[57] Ibíd.
[58] Por lo general el término usado en documentos internacionales es 'fichero*':* "fichero de datos personales: todo conjunto estructurado de datos personales, accesibles con arreglo a criterios determinados, ya sea centralizado, descentralizado o repartido de forma funcional o geográfica." [Directiva 95/46/CE literal c), artículo 2°]. El numeral 6, Artículo 4 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo adoptó la misma definición de la Directiva.

dado que su traducción a casos prácticos es de especial complejidad en la compresión de los retos del RGPDP.

Así mismo, es importante señalar que lo anterior tampoco se aleja de las definiciones que la academia le ha dado a las bases de datos desde hace unos 40 años. El Diccionario de Oxford de Informática entiende que el término de base de datos "[…] implica que cualquiera de los datos puede utilizarse como información clave para especificar consultas. En su acepción más común, esta expresión significa colección accesible de información, y en ese caso, sólo un conjunto limitado de valores de datos puede emplearse para especificar consultas."[59] En The Penguin Dictionary of Information Technology, una base de datos es definida de la siguiente forma: "en términos técnicos, un archivo estructurado de datos, esto es, un archivo conteniendo tanto datos como los medios para mantener las relaciones entre los datos."[60] El diccionario de español jurídico de la Real Academia Española la define en los siguientes términos: "Memoria informática en la que pueden integrarse datos dispuestos de modo que sean accesibles individualmente por medios electrónicos o de otra forma."[61] De forma similar define un fichero como un "Conjunto organizado de informaciones almacenadas en un soporte común."[62] Si bien todas las definiciones anteriores son predicables tanto de las bases de datos automatizadas como de las manuales o análogas, para efectos de este artículo se hará alusión máxime a las primeras.

El siguiente concepto central a toda la LEPD encontrado en el apartado objeto de estudio es el de tratamiento. La Constitución incluye este término en el segundo inciso del

[59] *Oxford Dictionary of Computing,* trad. Blanca de Mendizábal Allende, «base de datos»
[60] *The Penguin Dictionary of Information and Technology*, 3ra ed., «database»
[61] *Diccionario del español jurídico de la Real Academia Española,* «base de datos», acceso el 17 de enero del 2019, http://dej.rae.es/#/entry-id/E39570
[62] Ibíd., http://dej.rae.es/#/entry-id/E125260

artículo 15 indicando que: "En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución." La Ley 1581 de 2012 trajo una pequeña modificación al catalogar la recolección y circulación de datos, entre otras actividades, como especies del tratamiento de datos[63]. Así mismo, el desarrollo del concepto de tratamiento continúa la tendencia de acercarse a los estándares propuestos en la Resolución de Madrid en 2009[64] y por ordenamientos europeos[65]. Lo anterior también lo sostiene la Corte Constitucional cuando analiza la constitucionalidad del concepto de tratamiento diciendo que este "es de uso en el ámbito europeo y se encuentra tanto en la Directiva 95/46 del Parlamento Europeo como en los Estándares dictados en la reciente conferencia que se dio en Madrid […]"[66]. En síntesis, por tratamiento se entenderá cualquier operación manual o automatizada sobre datos personales.

Definidos estos últimos elementos de la segunda condición del ámbito de aplicación, se podrá estudiar la cuestión que gira en torno a las dificultades prácticas e interpretativas que trae el fragmento "registrados en cualquier base de datos que los haga susceptibles de

[63] "Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión." [Literal g) del artículo 3° de la Ley 1581 de 2012]

[64] Parte del objeto de la Resolución es "Definir un conjunto de principios y derechos que garanticen la efectiva y uniforme protección de la privacidad a nivel internacional, en relación con el tratamiento de datos de carácter personal […]" La Resolución de Madrid es también conocida por otros nombres como la Propuesta Conjunta para la Redacción de Estándares Internacionales para la protección de la Privacidad, en relación con el Tratamiento de Datos de carácter personal. En la 31ª Conferencia Internacional de la Protección de Datos y Privacidad, en la cual participaron más de 50 países, se plasmaron un conjunto de principios, derechos y obligaciones que si bien no tienen fuerza vinculante a nivel internacional, constituyen un instrumento importante de *soft law*. Además le sirve como referencia a países que para ese entonces no tenían un marco legal e institucional general en protección de datos como fue el caso de Colombia. En la sentencia C-748 de 2011, la Corte Constitucional hace varias referencias a lo acordado en dicha Conferencia.

[65] "Cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación, modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción." [Numeral 4 del Artículo 4° del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo]

[66] Corte Constitucional, STC C-748 de 2011, numeral 2.5.9.

tratamiento […]". El análisis se realizará a partir del planteamiento de situaciones tanto hipotéticas como reales que serán confrontadas con lo desarrollado hasta ahora. Finalizando se estudiará, en función de los interrogantes que irán apareciendo, una guía ofrecida por la Superintendencia de Industria y Comercio sobre el uso de sistemas de videovigilancia en el marco del RGPDP.

El primer escenario hipotético es el de un sistema complejo pero que como se verá más adelante está siendo implementado en Colombia. Las cámaras de este SV remiten las imágenes que capturan a computadores que cuentan con un software de identificación biométrica[67] a través del reconocimiento de patrones y características faciales de un individuo que lo distinguen de los demás. La información es luego almacenada y cotejada con imágenes de personas que fueron previamente ingresadas a una base de datos con el fin de verificar la identidad de estos individuos. A partir de ahí, dependiendo de la cantidad de información con la que cuente la base de datos o con qué otras bases se pueda comparar, se pueden realizar operaciones como consultar sus antecedentes judiciales o averiguar si es requerido por la justicia o alguna entidad[68].

[67] Biometría según la RAE: "Estudio mensurativo o estadística de los fenómenos o procesos biológicos." [*Diccionario de la Real Academia de la Lengua Española,* «Biometría», http://dle.rae.es/?id=5ZEB2lz]. Las tecnologías de biometría se valen de mecanismos de medición de características físicas o del comportamiento humano con el objetivo de determinar o autenticar su identidad.

[68] Si bien el enfoque ha sido el de vigilancia y fines similares, se han encontrado casos iguales o más preocupantes en los cuales estos sistemas se usan para fines comerciales. Un estudio conducido por la Comisión Federal de Comercio de los Estados Unidos (Federal Trade Comission o FTC) reveló un caso en el que una empresa de bebidas energéticas se había ingeniado una forma de publicidad en la cual un cartel digital tenía integrado una cámara que podía analizar el rango de edad y género de la persona observando. Así el cartel mostraba publicidad dirigida al consumidor basándose en la demografía del mismo. ["Facing Facts: Best Practices for Common Uses of Facial Recognition Technologies", en *Federal Trade Commission*, octubre del 2012, acceso el 17 de enero del 2019, https://www.ftc.gov/sites/default/files/documents/reports/facing-facts-best-practices-common-uses-facial-recognition-technologies/121022facialtechrpt.pdf

Es importante destacar algo de la idea anterior. Si un sistema está vinculado a una base de datos que cuenta con los registros de 500 personas, solo tendrá la capacidad de validar a través del software la identidad de dichos individuos. Dado el caso en que se capturen imágenes de alguien que no se encuentra registrado en dicha base, el computador no podrá identificarlo y sus fotografías o vídeos serán como las tomadas por cualquier otra cámara que no cuenta con tecnología de identificación biométrica.[69]

Puesto en los conceptos de la LEPD que se están manejando, los sistemas de videovigilancia descritos tratan datos personales que se encuentran registrados en una estructura organizada que permite el acceso a los mismos bajo criterios determinados de búsqueda. En el contexto internacional, constitucional y legal colombiano, las operaciones de los SV con software de identificación biométrica deben enmarcarse en los principios y las disposiciones de la ley especial de protección de datos personales.

Ahora bien, aún subsiste el escenario de las personas cuyas imágenes fueron capturadas por las cámaras pero cuyas identidades y datos no están registrados en las bases de datos de identificación biométrica. Algunos interrogantes emergen. ¿Por estar en el mismo archivo fílmico las imágenes de individuos registrados y no registrados hacen parte de la misma base de datos? ¿Componen horas interminables de grabaciones y datos crudos una base de datos? ¿Hasta dónde se puede llevar el concepto de *identificable* que trae la LEPD?

[69] "El tratamiento de fotografías no debe considerarse sistemáticamente tratamiento de categorías especiales de datos personales, pues únicamente se encuentran comprendidas en la definición de datos biométricos cuando el hecho de ser tratadas con medios técnicos específicos permita la identificación o la autenticación unívocas de una persona física." [Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, consideración 51.]

El caso del Sistema Integrado de videovigilancia Inteligente para Transmilenio (SIVIT) en Bogotá puede ilustrar mejor lo anterior. El primer trimestre de 2015 la Alcaldía Mayor de Bogotá, el Fondo de Vigilancia y Seguridad de Bogotá -hoy en día en proceso de liquidación- y la gerencia del Transmilenio anunciaron la adquisición de un novedoso sistema de videovigilancia que se instalaría en varios portales y estaciones. Dentro de la campaña publicitaria que se le hizo a las cámaras ante los medios de comunicación, Máximo Noriega Rodríguez, en ese entonces Gerente del Fondo, aseguraba que estas representaban un "salto tecnológico" para la seguridad del Transmilenio y que dichas cámaras eran capaces de identificar "[…] miles de rostros por segundo con más de 120 puntos de comparación" y que hacían parte de un "[…] esfuerzo de volver el Transmilenio en el sistema de transporte público más seguro de Latinoamérica."[70] Las cámaras con identificación facial[71] estarían conectadas a un centro de monitoreo que a su vez estaba vinculado a los celulares de la policía prometiendo así un tiempo de respuesta rápido a la hora de identificar y localizar a un sujeto de interés. En efecto, el sistema contratado con la firma americana FaceFirst es utilizado en varios aeropuertos y sitios con alto flujo de personas en el mundo. Pero como todos los sistemas con identificación facial, este necesita como prerrequisito una base de datos con la información biométrica de las personas a las que pretende hacerles seguimiento. Varios medios[72] de la ciudad denunciaron que las cámaras no estaban funcionando como se prometió, que el centro de monitoreo no estaba en operación y que la multimillonaria

[70] https://www.youtube.com/watch?v=lWoCC9IqNh0, acceso el 24 de enero del 2019

[71] Reconocimiento facial según el libro de Derecho & TIC 10.0: "Utiliza una cámara para tomar una foto del rostro de la persona. De la imagen se extraen elementos particulares (características relacionadas con las facciones) que luego se comparan con un banco de datos de imágenes en la que previamente está la foto de la persona que se busca identificar." [GECTI, *Derecho & TIC 10.0,* (Bogotá: Editorial Temis, 2011)]

[72] Redacción Bogotá, "Aún en veremos cámaras de reconocimiento facial para Transmilenio", *El Espectador,* 12 de junio del 2016, acceso el 17 de enero del 2019, https://www.elespectador.com/noticias/bogota/aun-veremos-camaras-de-reconocimiento-facial-transmilen-articulo-637688

inversión se había perdido. Sin embargo, el Fondo de Vigilancia se defendió argumentando que las cámaras estaban operando pero sin la modalidad de identificación biométrica que pronto estaría en funcionamiento. Esto obedece a dos factores. El primero es que la Alcaldía Mayor omitió detalles de cómo actúa el sistema ofrecido por FaceFirst cuando lo anunció al público. El segundo es que aún no existe la base de datos necesaria para que el sistema opere como se pensaba. De las más de 4.000.000 de personas que utilizan el Transmilenio al día, en junio de 2016 el Fondo de Vigilancia le dijo al Concejo de Bogotá que solo había 96 registros de prueba.

Entonces ¿Cómo enmarcar esta situación en función del aparte "[…] registrados en cualquier base de datos que los haga susceptibles de tratamiento […]"? Vale recordar que estas preguntas nacen de la aparente importancia que el legislador le concede a las bases de datos como un condicionante restrictivo dentro del ámbito de aplicación de la LEPD. ¿Será entonces que las filmaciones o imágenes capturadas de los usuarios del Transmilenio no registrados conforman una base de datos? Basándose en las definiciones aproximadas que se le dio a este tipo de bases de datos automatizadas, pareciera que no. No se puede acceder a la información personal contenida en los videos captados por las cámaras con arreglo a criterios de búsqueda determinados. Los datos no tienen una estructura organizada, estructura con la cual si cuenta la base de prueba. En otras palabras, los videos y las imágenes son datos crudos o datos primarios, entendidos estos como "datos en bruto; datos sin procesar. Datos en la forma que tienen cuando llegan al sistema informático desde el mundo exterior: los datos que no han sido reconocidos todavía para corregirlos, no se han clasificado en una secuencia, ni han sido procesados de ninguna otra manera."[73]. Incluso si los archivos fílmicos

[73] *Oxford Dictionary of Computing,* trad. Blanca de Mendizábal Allende, «datos en bruto»

fueran almacenados y organizados por fecha y hora, esto por sí solo no es un criterio para acceder a la información de una persona identificada o identificable. Se requiere de un análisis realizado por un ser humano o un software para volver esos datos crudos en información personal depurada o estructurada. En ese punto, para efectos de la LEPD, se podría hablar de una base de datos. ¿Se puede hablar entonces de bases de datos en potencia? Un caso común que puede dilucidar esta última idea es en el que posterior a un hurto las autoridades o quien tenga acceso a las cámaras consultan las grabaciones de cámaras de vigilancia cercanas. Además de surtir a los noticieros del medio día con contenido, las filmaciones son usadas para intentar identificar al delincuente. Lo que en su momento fue un cúmulo de datos caóticos, ahora tiene algo como 'vocación' de base de datos.

De igual forma se encuentran los sistemas de videovigilancia que no cuentan con un sistema de almacenamiento. Consisten en cámaras que reproducen en tiempo real las imágenes que capturan. Al no tener la capacidad de almacenar lo que registran, no pueden generar bases de datos. La información que reproducen desaparece al instante. En ese orden de ideas, teniendo en consideración únicamente el aparte objeto de estudio, la conclusión lógica sería descartar del ámbito de aplicación de la LEPD este tipo de sistemas, - en lo que a disposiciones corresponde - toda vez que la segunda condición exige que los datos personales deben estar registrados en una base de datos. Bajo ese supuesto, actualmente hay una cantidad incalculable de cámaras de bajo costo en funcionamiento captando información personal y lo que los llama a tener un manejo responsable de estos datos son los principios y garantías que ya habían sido sistematizados sin necesidad de la LEPD.

En la misma línea, la literalidad del parágrafo[74] del artículo en estudio cae en la misma 'trampa' del lenguaje utilizado en la redacción de la LEPD. El aparte amplía el ámbito de aplicación de los principios desde las bases de datos, no desde las actividades de tratamiento por sí solas. Sin embargo de acuerdo a lo expuesto en el capítulo sobre los principios, la jurisprudencia de la Corte Constitucional indica que el deber de respetar los principios de la administración de datos no obedece a la existencia de una base de datos ni su finalidad sino únicamente al tratamiento de datos.

Ultimando, como se dijo en la introducción a este título, con el fin de "brindar orientación a quienes implementen SV […]"[75] la Superintendencia de Industria y Comercio pública en septiembre de 2016 una guía titulada *Protección de datos personales en sistemas de videovigilancia*. En esta, según el mismo documento se "precisan algunos aspectos que deberían ser tenidos en cuenta para garantizar la protección de los derechos de los Titulares [sic] de información cuyas imágenes son captadas mediante SV."[76] Al momento de esclarecer cuándo un sistema de videovigilancia queda sujeto al RGPDP, la guía se aleja de lo establecido en la ley. En ella se lee que: "en el caso de las imágenes de personas determinadas o determinables, operaciones como la captación, grabación, transmisión, almacenamiento, conservación, o *reproducción en tiempo real* o posterior, entre otras, son consideradas como Tratamiento de datos personales, *y en consecuencia, se encuentran sujetas al Régimen*

[74] "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 e manera concurrente a los previstos en la presente ley."[Parágrafo del artículo 2° de la Ley 1581 de 2012]

[75] Superintendencia de Industria y Comercio, *Protección de datos personales en sistemas de videovigilancia,* septiembre del 2016, pág. 4, acceso el 17 de enero del 2019, http://www.sic.gov.co/sites/default/files/files/Nuestra_Entidad/Guia_Vigilancia_sept16_2016.pdf.

[76] Ibíd.

General de Protección de Datos Personales." [Itálicas nuestras][77]. Se evidencia en el fragmento cómo se omite el requisito del registro de los datos personales en una base de datos. La guía plantea una relación de causalidad suficiente entre la presencia de actividades de tratamiento y la sujeción al RGPDP, lo cual va en contravía con lo preceptuado en el artículo 2º de la Ley 1581 que como se ha señalado en reiteradas ocasiones, impone tres condiciones.

Es evidente que la SIC no posee la potestad reglamentaria en sentido formal que tiene el Presidente de la República o los Ministerios de forma residual y subordinada respecto al primero. Tampoco se puede concluir que el literal e)[78] del artículo 21 de la LEPD le confiere potestad reglamentaria a la Superintendencia. Las instrucciones impartidas deben ajustar las operaciones de quienes realicen tratamiento a lo establecido en el RGPDP. Inferir que de la literalidad de dicha disposición se le otorga potestad reglamentaria a la SIC llevaría a interpretaciones del "espíritu de la norma" o a invocar argumentos parecidos y recurrentes en situaciones mucho más complicadas de interpretación normativa.

Por su parte la Corte Constitucional de manera breve señala que las funciones conferidas en el artículo "[…] desarrolla[n] las funciones de vigilancia del cumplimiento de la normativa, de investigación y sanción por su incumplimiento, de vigilancia de la transferencia internacional de datos y de promoción de la protección de datos."[79] En ningún

[77] Ibíd., 5

[78] "Impartir instrucciones sobre las medidas y procedimientos necesarios para la adecuación de las operaciones de los Responsables del Tratamiento y Encargados del Tratamiento a las disposiciones previstas en la presente ley."

[79] Corte Constitucional, STC C-748 de 2011, numeral 2.20.3.

momento la Corte se refiere a la facultad de reglamentar o a la intención del legislador de conferirla, lo cual se esperaría en un análisis de constitucionalidad si así fuese el caso.

Por otro lado, el debate alrededor de si las disposiciones de algunas autoridades – en este caso la mencionada guía – son fuente de derecho administrativo se aleja del asunto principal de nuestra investigación[80]. Aun así, si se aceptase en gracia de discusión que una guía es fuente de derecho administrativo porque crea una situación jurídica para los administrados aún en contravía de lo que dispone una ley estatutaria en su ámbito de aplicación, subsiste un problema. Dicha guía no fue publicada en el Diario Oficial o en su equivalente en la SIC, el Boletín Jurídico, contrario a las demás circulares, conceptos y resoluciones de la entidad. Por lo que aun aceptando todo lo anterior, no se estaría cumpliendo el principio de publicidad y por lo tanto, el acto es inoponible. Sin embargo, el literal i)[81] del mismo artículo 21 le confiere una herramienta a la Superintendencia para que, si considera la normatividad actual insuficiente y que por lo tanto debe ser modificada, los órganos competentes sean quienes realicen dichos ajustes. Esta sería la herramienta idónea partiendo de la tesis de que en efecto la SIC consideró la redacción del artículo 2 de la LEPD desafortunada y desea cobijar sin lugar a duda formas de tratamiento como las de las cámaras que transmiten en tiempo real. Cabe resaltar que desde el punto de vista práctico, las guías, cartillas y publicaciones similares de la SIC son muy bien recibidos por el sector empresarial y abogados practicantes por provenir directamente de una institución técnica y especializada.

[80] A modo de anécdota, Mariano Baena Alcázar plantea un interesante análisis de derecho comparado sobre dicho tema en su texto *Instrucciones y Circulares como fuente del derecho administrativo*. Y es precisamente la Instrucción 1/2006 de la Agencia Española de Protección de Datos, publicada en el Boletín Oficial del Estado, la que antecedió a la Guía de videovigilancia de la misma entidad. [Mariano Alcázar, "Instrucciones y Circulares como fuente del derecho administrativo", en *Revista de administración pública*, n°48, (1965), 107-126].

[81] "Sugerir o recomendar los ajustes, correctivos o adecuaciones a la normatividad que resulten acordes con la evolución tecnológica, informática o comunicacional."

El rigor – tal vez exegético – al analizar ese último escenario tedioso pretende señalar el problema que representa edificar en gran parte la aplicabilidad del RGPDP sobre el concepto de base de datos. Este diseño pone en una zona privilegiada formas de explotación y usos de datos personales cuya regulación debería ser más determinable. Como son las cámaras que transmiten en directo pero no realizan grabación alguna. El reproche o reclamo que se le hace al legislador apunta al caos innecesario que produce su excesiva ambigüedad. El desarrollo internacional en protección de datos es relativamente uniforme y accesible para adaptarse a un ordenamiento jurídico. La Corte Constitucional ya tenía un desarrollo amplio influenciado por la Directiva 95/46/CE y para ninguno las bases de datos eran un elemento central. Tendencia que ha sido mantenida en el Reglamento (UE) 2016/679.

Los problemas al conciliar la videovigilancia y al RGPDP no se limitan a la hermenéutica o a ambigüedades en el lenguaje. Se procederán a abordar los siguientes asuntos que contribuyen a dibujar la aseveración anterior: (i) el tratamiento de datos sensibles; (ii) el ámbito temporal del tratamiento de datos y (iii) la autorización del titular. Los tres temas se ajustan a cualquier tipo de sistema de video-vigilancia, pero la estructura a través de la cual se explicarán será principalmente desde dos casos. El primero es el del Transmilenio que fue expuesto en el capítulo pasado. El segundo es el de un sistema de videovigilancia impulsado por varias instituciones del gobierno que se está implementando en diferentes escenarios deportivos del país.

El tratamiento de datos sensibles y los excesos de la videovigilancia

Aquellos datos personales que pueden exponer a los titulares a una situación de discriminación o vulnerabilidad tienen una relación estrecha con el núcleo esencial del derecho a la intimida, por lo que merecen protección especial. La LEPD define los datos sensibles en su artículo 5 de la siguiente manera:

> […] [S]e entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición así como los datos relativos a la salud, a la vida sexual y los datos biométricos.

La Corte Constitucional cataloga los datos sensibles como "reservada o secreta" porque guardan "estrecha relación con los derechos fundamentales del titular – dignidad, intimidad y libertad – se encuentra reservada a su órbita exclusiva y no puede siquiera ser obtenida ni ofrecida por autoridad judicial en el cumplimiento de sus funciones."[82]

Los datos que se consideran de naturaleza sensible o reservada en palabras de la Corte "[…] son determinados por los cambios y el desarrollo histórico."[83]. Esta aseveración puede tener diferentes explicaciones. Una es el progreso en la protección de derechos humanos a la hora de responder a fenómenos de discriminación o marginación que se han dado a lo largo de la historia. Otra es la aparición de nuevas tecnologías que permiten recolectar datos que en algunas ocasiones se clasifican como sensibles. Lo anterior quiere decir, y así lo ha sostenido la Corte en reiteradas ocasiones, que las listas de datos sensibles contenida en la ley son enunciativas y no taxativas.

Las tecnologías al servicio de la seguridad y la vigilancia cada vez hacen mayor uso de datos que caen dentro de esta categoría como es el caso de los datos biométricos. Esto se debe, entre otras cosas, a que pueden proveer información más detallada y confiable a la hora de identificar individuos de su interés. Sin embargo cada vez es más frecuente ver dispositivos con sistemas de identificación biométrica en distintos lugares donde la necesidad de dicha tecnología es cuestionable. Es probable que el aumento se atribuya a varios factores como la mayor accesibilidad a estas tecnologías, la necesidad de sistemas de seguridad más confiables o al simple capricho de tener tecnología de punta. Si bien se hablará principalmente de la identificación biométrica por ser de vanguardia, la recolección de datos

[82] Corte Constitucional, STC T-729 de 2002. C-336 de 2007 y C-334 de 2010.
[83] Corte Constitucional, STC C-748 de 2011, numeral 2.7.3.

sensibles por parte de entidades de seguridad no es un fenómeno nuevo. Puede haber casos donde los sistemas de seguridad también graben sonidos y se recolecten conversaciones de personas sobre diversos temas íntimos como su orientación sexual, su religión o preferencias políticas.

La carnetización obligatoria de los asistentes a los estadios de fútbol acompañado de la instalación de sistemas de videovigilancia en varias ciudades del país es un ejemplo que será clave para hacerse una idea sobre cuál será la tendencia los próximos años. Por medio de la Ley 1270 de 2009 y el Decreto 1717 de 2010 se determinó necesario crear la Comisión Nacional de Seguridad, Comodidad y Convivencia en el Fútbol. La Comisión está compuesta por representantes de diferentes organismos e instituciones del Estado de orden nacional, territorial y representantes del gremio. La idea es estructurar una serie de estrategias y planes a nivel nacional y local para solucionar los problemas que se dan dentro y fuera de escenarios deportivos. Si bien la Comisión ha escuchado las voces de la academia y de la ciudadanía para buscar soluciones diferentes a la acción de la fuerza pública, el *dataveillance* y la videovigilancia entran a jugar un papel clave. Dentro de las funciones que la ley le confirió a la Comisión están:

> 4. Diseñar y promover un sistema de registro que les permita a los clubes de fútbol profesional contar con información actualizada de los miembros de sus barras. En este registro deberá figurar, por lo menos, el nombre completo, la cédula de ciudadanía o tarjeta de identidad y *la profesión u ocupación de cada integrante*, estos datos deberán ser confrontados con los documentos que sustenten la veracidad de dicha información. Al momento de la inscripción, el club entregará una credencial o carné numerado, individual e intransferible, que

contenga los citados datos y una fotografía reciente, y que, en la medida de lo posible, dificulte su adulteración."[84] [Itálicas nuestras]

De manera posterior, el Ministerio de Interior expidió el *Protocolo para la seguridad, comodidad y convivencia del fútbol*. En este documento, la Comisión le delega a la División Mayor del Fútbol Profesional Colombiano (DIMAYOR) el diseño e implementación de dicho sistema[85]. En la misma línea con el artículo citado, el *Protocolo* establece lo siguiente:

> 5.8.22.1 DATOS FUNDAMENTALES CARNETIZACIÓN. En el artículo tercero, numeral 4 de la ley 1270, se establecen como requisitos mínimos: Nombre completo, documento de identidad, teléfonos de contacto, dirección domicilio, dirección trabajo, profesión y ocupación. El club debe entregar el carné numerado con los datos citados y una foto reciente. El sistema de carnetización *podrá incluir sistema de huellas dactilares*. Estos son los mínimos exigidos, sin embargo es necesario ampliar la información de los aficionados *sobre todo de los que integran las barras que se ubican en las tribunas populares*, ya que se argumenta una problemática social la cual, soportada desde una información mínima, puede tener repercusión en las políticas de inversión a nivel nacional y local para los diferentes grupos poblacionales. En este sentido, *se debe considerar: nivel escolar, estrato social, nivel educativo, afiliación a sistema de salud, composición familiar, tipo de vivienda, edad, género, y datos de ubicación, entre otros."* [Itálicas nuestras]

[84] Ley 1270 de 2009, artículo 3, numeral 4.
[85] Anexo técnico No. 1 del Decreto 1717 de 2010, Protocolo para la seguridad, comodidad y convivencia del fútbol, numeral 5.8.22

En síntesis, a la DIMAYOR se le delegó crear una base de datos que tenga registrada información sobre las personas que acuden a los partidos de fútbol y que en coordinación con los equipos, se obligue a todas las hinchadas a identificarse mediante carné o tarjeta oficial.

Así es como los alcaldes de Medellín en un aparente afán de obtener otro reconocimiento internacional, entraron a la competencia de ciudades con mayor cantidad de cámaras de videovigilancia. El secretario de seguridad de la ciudad, Andrés Felipe Tobón, dijo en entrevista con el diario El Colombiano, que el Estadio Atanasio Girardot cuenta con 170 cámaras con un sistema de identificación facial integrado[86]. Desde el primer semestre de 2018, ya es obligatorio para las tribunas populares de la ciudad portar el carné que identifica a los hinchas. Para el caso de todos los hinchas de Atlético Nacional, el documento debió ser tramitado con el equipo directamente, el cual contrató el servicio de logística con la empresa Tu Boleta (Ticket Fast S.A.S.). Por otro lado, los hinchas abonados del Deportivo Independiente Medellín no tuvieron que realizar ningún trámite porque el equipo ya tenía la información que la DIMAYOR necesitaba[87]. Para el caso del primer equipo, los hinchas debían proveer, aparte de algunos datos generales, sus huellas dactilares y fotografías de sus rostros. Suponiendo que dichas fotos sean óptimas como referencia para que las cámaras de identificación facial puedan determinar o autenticar la identidad de las personas, son dos datos biométricos (sensibles), que se estarían exigiendo para ir a ver fútbol.

[86] Daniel Henao, "Carnetización obligatoria para frenar inseguridad en estadios", *El Colombiano,* 21 de julio del 2017, acceso el 17 de enero del 2019, http://www.elcolombiano.com/deportes/futbol-colombiano/carnetizacion-obligatoria-de-hinchas-en-colombia-para-frenar-inseguridad-en-estadios-DD6948335

[87] Uno de los puntos grises alrededor de este tema es cómo fue el trato entre la DIMAYOR y este equipo. La calidad de la información, el mecanismo legal y si los abonados autorizaron una posible transferencia masiva de información personal es desconocido.

Basarse en que este tipo de medidas se han implementado en otros países con historia de violencia en los estadios como el Reino Unido y que por ende deberíamos seguir su ejemplo no es del todo satisfactorio. En parte porque los resultados no se dan sin políticas sociales que las acompañen, como sucede en Argentina donde los mismos problemas subsisten. Además si cualquier error de diseño lleva a una base de datos a vincular personas incorrectas, el daño puede ser catastrófico. Por ejemplo, asumiendo que la población en Colombia es de 45 millones de personas, aun un sistema con un nivel de precisión del 99.9%, pondría a 45 mil colombianos en riesgo de encajar en algún perfil erróneo de un algoritmo. Si esto será aceptable podrá depender de quienes sean esos 45 mil afectados. Finalmente las normas que protegen los datos sensibles en Colombia tienen particularidades que las distancian de las encontradas en ordenamientos de otros países.

Tal es el caso del segundo contenido normativo artículo 6 del Decreto 1377 de 2013[88]. Al final del artículo se dispone que: "Ninguna actividad podrá condicionarse a que el Titular suministre datos personales sensibles." Prohibición que la Corte estima es "una garantía del *habeas data* y del derecho a la intimidad, y además se encuentra estrechamente relacionada con la protección de la dignidad humana."[89] La disposición no ha estado libre de crítica y cuestionamientos. El Superintendente delegado para la protección de datos personales Nelson Remolina Angarita[90] argumenta que la prohibición podría generar inconvenientes para el mismo titular del dato. El autor pone casos en los que el uso de estos datos es indispensable como al momento de recibir atención médica. Crítica válida por los bienes jurídicos en riesgo. Pero también se puede pensar en las entrevistas de trabajo en las que

[88] Por el cual se reglamenta parcialmente la Ley 1581 de 2012.
[89] Corte Constitucional, STC C-748 de 2011, numeral 2.8.4.
[90] Nelson Angarita, *Tratamiento de datos personales: aproximación internacional y comentarios a la ley 1581 de 2012,* (Bogotá: Legis Editores S.A., 2013).

preguntan información sensible sin relación con el cargo. Esos espacios relativos a las excepciones y las tensiones entre el *habeas data* y otros principios son los que el legislador estatutario debe desarrollar.

El precepto es muy contundente. No está escrito de manera que permita leerse con matices que den lugar a un debate interpretativo. Tampoco se encuentran disposiciones similares en ningún otro ordenamiento, lo cual no deja de ser extraño dada la fuerte influencia que la regulación europea tuvo sobre la redacción de la LEPD. Lo cierto es que hasta hoy sigue vigente sin ninguna modificación.

La prohibición definitivamente merece más desarrollo y profundidad. Hay casos en los que la recolección de dichos datos es un condicionante como el de la DIMAYOR. En este el acceso a los estadios está condicionado a que cada individuo suministre por lo menos un dato sensible – su huella dactilar –. Lo mismo se puede decir de las cámaras del Transmilenio si hubiesen sido instaladas e implementadas correctamente. Para el primero, hoy se podría presentar un reclamo ante la Superintendencia de Industria y Comercio por la infracción de lo dispuesto en el Decreto 1377. Hay otros casos en los que no se condiciona ninguna actividad al suministro de datos sensibles, sin embargo se recogen sin autorización o conocimiento del titular y a veces incluso del Responsable o Encargado como es la grabación de conversaciones privadas a través de un sistema de seguridad con videocámaras y micrófonos. Los ejemplos dados son apenas las pruebas de una inversión de por lo menos veintiséis mil millones de pesos (COP $26.000.000.000) anunciada por el Ministerio de Interior en diciembre de 2016 para instalar cámaras de seguridad, algunas de ellas con

identificación biométrica y vincularlas con bases de datos de la fuerza pública[91]. La prohibición debe ser desarrollada antes de que estos sistemas entren de forma rápida y silenciosa a diferentes esferas y la ciudadanía lo asimile como algo normal y necesario. A la fecha de la entrega de este trabajo no se encontró ningún reclamo, queja resuelta u otro pronunciamiento de la SIC al respecto.

[91] Comunicado de Prensa, "Antes de finalizar 2017 Sistema de Identificación Biométrica ABIS estará en todo el país: MinInterior", 19 de diciembre del 2016, acceso el 17 de enero del 2019, http://www.legisaldia.com/BancoMedios/Archivos/comunicado-antesdefinalizar2017sistemadeidentificacionbiometricaabisestaraentodoelpaismininterior-16.pdf

El ámbito temporal y funcional del tratamiento de datos personales en la vigilancia

¿Qué sucede si los sistemas de vigilancia resulten ser innecesarios, ineficaces o inútiles? La instalación y la operación de estos sistemas deberían obedecer a evaluaciones o estudios de impacto previos y posteriores de idoneidad, necesidad y proporcionalidad. ¿El sistema es susceptible de lograr el objetivo propuesto? ¿Existe otro medio menos invasivo para la consecución de los propósitos? ¿De la implementación del sistema se derivan más beneficios para el interés general que perjuicios sobre otros bienes en conflicto? ¿Cuál es el grado de expectativa de privacidad en esas circunstancias? Incluso si en principio la vigilancia que usa datos sensibles supera estas preguntas de viabilidad, en el futuro puede demostrar no ser funcional al hacer los mismos juicios. Si los sistemas de vigilancia fuesen sometidos a estos criterios de la misma forma que son analizados sus beneficios económicos, seguramente muchos no serían instalados y otros serían retirados.

El ejemplo del sistema de carnetización y vigilancia de la DIMAYOR en Medellín sirve para ilustrar lo anterior. La idea de exigir el carné a partir del inicio del año 2018 y la instalación de las cámaras en el Atanasio Girardot, era poder identificar e individualizar a aquellos sujetos que incurrieran en conductas prohibidas o indebidas para sancionarlos. Lo anterior solucionaría un problema recurrente que era la sanción de tribunas enteras por el comportamiento de pocos individuos. Un sistema de videovigilancia con identificación facial y una base de datos con la información biométrica de todos los hinchas fue la solución estimada como ideal. Sin embargo, mediante la Resolución No.002 de 2018, la entidad sancionó a Atlético Nacional con dos fechas de suspensión parcial a las tribunas sur y

occidental por la conducta de unos pocos. En mayo otro evento similar dio lugar a la misma sanción.

Independientemente de las causas, el hecho es que el sistema no está funcionando. Las sanciones siguen siendo para todos los asistentes de la tribuna 'involucrada'. Y si bien las razones pueden ser técnicas[92] y remediables, algunas de las mismas barras objeto de vigilancia, en conjunto con las autoridades locales, pueden volver esos sistemas innecesarios.

La barra Los del Sur, hinchas de Atlético Nacional lleva varios años realizando procesos de cambio que han traído resultados ejemplares. La barra se estructuró y organizó de tal forma que desde 2016 cuenta con su propio equipo de logística encargado de ese trabajo en la tribuna sur. Este está conformado por personas que tienen dificultades en sus hogares o que por diferentes motivos no pueden conseguir empleo. El equipo de logística no solo observa que el ingreso al estadio se haga de manera ordenada y civilizada, si no que también, junto a algunos dirigentes de la barra, son los encargados de evitar y resolver los conflictos que se dan en la tribuna. La identificación común y el grado de aceptación es tal que la policía ya no tiene presencia en este sector debido al respeto que los hinchas le tienen a esta logística y a los líderes.

Así mismo, desde los dos clubes de fútbol de la ciudad, las barras y la Alcaldía han impulsado varias campañas de convivencia[93] que han logrado reducir las cifras de violencia

[92] No es posible corroborarlo ni se han hecho anuncios, pero en mi opinión las fotos que se le tomaron a los aficionados no sirven. Lo anterior porque los sistemas de identificación facial se valen de cientos de puntos de referencia en el rostro, y es muy probable que las fotos tomadas no aporten suficientes 'puntos'. Esto, sin embargo, no deja de ser apenas una apreciación personal sin valor científico.

[93] Medellín, "El balón rodará 24 horas continuas en Medellín por un fútbol en paz", *El Tiempo*, 5 de abril del 2018, acceso el 17 de enero del 2019, http://www.eltiempo.com/colombia/medellin/el-balon-rodara-24-horas-continuas-en-medellin-201726

dentro y fuera del estadio. Y aunque para los habitantes de Medellín es normal que las tribunas no cuenten con barreras, esto es la regla en el resto del mundo.

¿Entonces para que serán las cámaras si no para ser testigos mudos de la violencia? ¿Contribuyen de verdad a un mejor ambiente? Después de todo, las cámaras son medidas reactivas que nada pueden hacer en el momento que se dan los incidentes. ¿Para qué políticas tan invasivas cuando otras aproximaciones sociales han mostrado resultados positivos? Las iniciativas expuestas son más democráticas que el sistema de vigilancia más refinado y moderno. Bien podrían dejarse apagadas y cumplirían una función disuasiva y poco invasiva.

Si la cultura de la convivencia pacífica se interioriza, presumiendo que el fin de las cámaras, la base de datos, y la recolección de datos sensibles es únicamente la seguridad, ¿cuál es el punto de dejar el sistema de vigilancia operando? Y llevándolo al plano de los sistemas de videovigilancia en general, ¿la idea es dejarlos indefinidamente o en algún momento se confiará en el civismo de los ciudadanos?

El Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo si tuvo en consideración varios de estos planteamientos. Estimaron que pueden entrañar un alto riesgo para los derechos y libertades de las personas las operaciones de tratamiento que implican el uso de nuevas tecnologías sin la realización de una evaluación previa de impacto a la protección de datos, o si resultan necesarias después de un tiempo.[94] Por lo anterior, el Reglamento prescribe que deben hacerse evaluaciones de impacto cuando "sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas físicas,

[94] Consideraciones 89, 90, 91 y 92 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo.

el responsable del tratamiento realizará, antes del tratamiento, una evaluación de impacto de las operaciones de tratamiento en la protección de datos personales."[95] Algunos casos en los que el Reglamento exige evaluaciones de impacto son en la observación sistemática a gran escala de una zona de acceso público y en los que se elaboran perfiles a través de un tratamiento automatizado y exhaustivo de datos personales que sean base para tomar decisiones que produzcan efectos jurídicos para personas naturales o los afecten de manera similar.[96]

Para que Colombia esté al nivel de los compromisos y directrices en protección de datos personales de los demás estados que hacen parte de la OCDE[97] y sea fiel a los lineamientos y principios constitucionales, la SIC debería recomendar que el RGPDP se actualice en este sentido. Con el acompañamiento de las autoridades de control, se debería evaluar el impacto real que están teniendo las políticas de seguridad que se valen de nuevas tecnologías y de sistemas automatizados (tanto públicas como privadas) que pueden vulnerar los derechos y libertades de los ciudadanos.

Sin embargo el RGPDP trae una norma que puede servir como una base más o menos sólida para enfrentar la implementación excesiva e indiscriminada de sistemas de vigilancia automatizados: el artículo 11 del Decreto 1377 de 2013, que reglamenta el límite temporal que tienen las actividades de tratamiento de datos personales[98]. Bajo los criterios de

[95] Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, sección 3, artículo 35, numeral 1.
[96] Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, sección 3, artículo 35.
[97] "[…] los países miembro tienen un interés común en proteger la intimidad y las libertades individuales, y en reconciliar los valores fundamentales en oposición, tales como la intimidad y la libre circulación de información." [Sección de "reconocimientos" de la Recomendación del Consejo de la OECD relativa a las directrices que rigen la protección de la intimidad y de la circulación transfronteriza de datos personales, 23 de septiembre de 1980]
[98] "Los Responsables y Encargados del Tratamiento solo podrán recolectar, almacenar, usar o circular los datos personales durante el tiempo que sea razonable y necesario, de acuerdo con las finalidades que justificaron el tratamiento, atendiendo a las disposiciones aplicables a la materia de que se trate y a los aspectos

razonabilidad y necesidad, una vez cumplida la finalidad que dio lugar al tratamiento de datos personales, estos deben ser suprimidos. Esto lleva a preguntarse, más allá de la sola supresión, si al momento de diseñar una política de seguridad que se vale de tecnologías como la videovigilancia y el tratamiento de datos, los que la implementan prevén un escenario – o si está dentro de sus expectativas – en el que este podría dejar de ser necesario. Desde la perspectiva de los vigilados y los titulares de los datos, no es descabellado pensar que la promesa de dejar de ser observados y perfilados pueda ser un incentivo para que, al menos en lugares como un estadio y otros escenarios públicos, el comportamiento de la ciudadanía cambie.

administrativos, contables, fiscales, jurídicos e históricos de la información. Una vez cumplida la o las finalidades del tratamiento y sin perjuicio de normas legales que dispongan lo contrario, el Responsable y el Encargado deberán proceder a la supresión de los datos personales en su posesión. No obstante lo anterior, los datos personales deberán ser conservados cuando así se requiera para el cumplimiento de una obligación legal o contractual."

Autorización

Como regla general, el tratamiento de datos es legitimado cuando media una autorización del titular de los datos. Dicha legitimación se origina en el principio de libertad, el cual prescribe que el tratamiento de datos personales "[…] solo puede ejercerse con el consentimiento previo, expreso e informado del titular."[99] El concepto de consentimiento, una manifestación libre de la voluntad, es un elemento esencial, un pilar sobre el que se levanta la defensa de los derechos a la autodeterminación informática, el *habeas data* y la intimidad.

La autorización se caracteriza por ser previa, expresa e informada. El tratamiento de datos personales legítimo está condicionado a estos tres elementos del consentimiento[100]. Por un lado, está el carácter previo, que no es más que es una condición de temporalidad. En pocas palabras, se debe obtener la autorización del titular del dato en un momento anterior al tratamiento. Por otra parte, el carácter expreso significa que el consentimiento debe ser otorgado de forma inequívoca y con absoluta claridad. Esto hace que no sea "[…] posible aceptarse la existencia, dentro del ordenamiento jurídico colombiano, de un consentimiento tácito."[101] Para la Corte esto se traduce "en la prohibición de otorgarse autorizaciones abiertas y no específicas."[102] Finalmente el carácter informado busca que el titular tenga pleno conocimiento sobre varios asuntos para que pueda tomar una decisión a consciencia. El

[99] Ley 1581 de 2012, artículo 4, literal c.
[100] "[…] la legitimidad constitucional de los procesos de acopio, tratamiento, y divulgación de datos personales se sustenta, entre otros aspectos, en que el sujeto concernido preste su autorización libre, previa y expresa." [STC C-1011 de 2008, numeral 3.2.2.2]
[101] STC C-1011 de 2008, numeral 2.6.5.2.3
[102] STC C-1011 de 2008, numeral 2.6.5.2.3

artículo 12 de la Ley 1581 establece que a la hora de solicitar la autorización del titular, el responsable:

> [D]eberá informarle de manera clara y expresa lo siguiente: a) el tratamiento al cual serán sometidos sus datos personales y la finalidad del mismo; b) el carácter facultativo de la respuesta a las preguntas que le sean hechas, cuando estas versen sobre datos sensibles o sobre datos de las niñas, niños y adolescentes; c) los derechos que le asisten como Titular; d) la identificación, dirección física o electrónica y teléfono del Responsable del Tratamiento.

De esta forma es como juntos, el requisito temporal (previo), de forma (expreso) y de fondo (informado) del consentimiento, constituyen un ejercicio de la libertad del individuo en la administración de sus datos personales. Es decir, la potestad en cabeza del individuo de decidir libremente qué hacer con su información. La ausencia de una de las 3 condiciones, por regla general, invalida el tratamiento de esos datos y puede dar lugar a sanciones por parte de la Superintendencia de Industria y Comercio.

La Ley 1581 también contempla algunos casos en los que no se necesita autorización de los titulares para tratar sus datos personales. La limitación al principio de libertad en los casos exceptuados, se justifica en la protección a otros bienes jurídicos o la existencia de intereses constitucionales. La primera excepción es probablemente la de mayor relevancia para este texto. Esta prevé que la autorización no será necesaria cuando se trate de "Información requerida por *entidad pública o administrativa en ejercicio de sus funciones legales* o por orden judicial."[103] [Itálicas nuestras]

[103] Ley 1581 de 2012, artículo 10, literal a.

En este sentido, en el estudio del proyecto de la referida ley, la Corte Constitucional se remitió a las observaciones realizadas en la Sentencia C-1011 de 2008, que revisó la Ley 1266 de 2008. La Corte consideró que el literal d) del artículo 5º [104] no es una condición en extremo abierta o indefinida. Así, para garantizar la eficacia del derecho al *habeas data* y procurar que dicha excepción no se convierta en una herramienta proclive al abuso del poder informático por parte del Ejecutivo, la Corte identificó dos condiciones:

> (i) el carácter calificado del vínculo entre la divulgación del dato y el cumplimiento de las funciones de la entidad del poder Ejecutivo; y (ii) la adscripción a dichas entidades de los deberes y obligaciones que la normatividad estatutaria predica de los usuarios de la información, habida consideración que ese grupo de condiciones permite la protección adecuada del derecho.[105]

Por lo tanto las actividades de tratamiento de datos por parte de entidades (públicas o administrativas) del Ejecutivo devendrán legítimas en la medida que haya un vínculo o una relación clara entre el tratamiento y las funciones de la entidad. Además deberán cumplir con los demás principios y garantías propios del *habeas data.*

Lo anterior probablemente exime de la obligación de solicitar autorización a la mayoría de las actividades de videovigilancia que involucren a la Fuerza Pública. Si bien el término para referirse a los organismos nacionales de seguridad no es precisamente 'entidad', sí están subordinadas o son dependientes del Poder Ejecutivo[106]. Por lo que se puede asumir

[104] "La información personal recolectada o suministrada de conformidad con lo dispuesto en la ley a los operadores que haga parte del banco de datos que administra, podrá ser entregada de manera verbal, escrita, o puesta a disposición de las siguientes personas y en los siguientes términos: d) A las entidades públicas del poder ejecutivo, cuando el conocimiento de dicha información corresponda directamente al cumplimiento de alguna de sus funciones."

[105] Corte Constitucional, STC C-748 del 2011, numeral 2.12.3.

[106] Constitución Política de Colombia, capítulo 7, artículo 216.

que también son incluidos en la excepción. Sea un plan impulsado desde el Ministerio de Interior, una orden de una administración municipal o una estrategia diseñada por la Comisión, lo más probable es que quien lidere y organice la operación sea un comando o dependencia de la Policía Nacional. En últimas el Responsable del tratamiento que para este efecto en quien normalmente recaería la obligación de recoger la autorización, seguramente sea del Ejecutivo. Siendo así, sin duda tendrá funciones que están directamente relacionadas con la seguridad del pueblo, dando por cumplida la primera de las dos condiciones mencionadas anteriormente. En el marco de la seguridad y la videovigilancia, esto evita la dificultad logística o de ejecución como es que el Estado recoja las autorizaciones de quienes constitucionalmente está llamado a proteger.

A su vez, "la adscripción a dichas entidades de los deberes y obligaciones que la normatividad estatutaria predica […]"[107] es un requisito que brinda confianza al reafirmar que deben enmarcarse en los demás principios como finalidad, confidencialidad y seguridad. Además provee a las personas de herramientas para protegerse de los abusos que se le pueden dar a sus datos. Una lectura integral de los artículos 14 y 15 de la LEPD, dispone que una persona legitimada podría elevar una consulta[108] o reclamo sobre la información suya que reposa en las bases de datos del Responsable, sea este un privado o público.

El principio de libertad presenta más retos para las demás personas jurídicas que operan sistemas de videovigilancia. La Guía ofrece unas bases de implementación entre las

[107] Corte Constitucional, STC C-748 del 2011, numeral 2.12.3.

[108] Ley 1581 de 2012, Artículo 14: "Los Titulares o sus causahabientes podrán consultar la información personal del Titular que repose en cualquier base de datos, sea esta del sector público o privado. El Responsable del Tratamiento o Encargado del Tratamiento deberán suministrar a estos toda la información contenida en el registro individual que esté vinculada con la identificación del Titular."

que está el consentimiento de las personas como un factor a tener en cuenta al operar cámaras de videovigilancia. Sin embargo se siente incompleta y desactualizada.

El modo de obtener la autorización de todas las personas cuyos datos sean capturados por el lente de una cámara de vigilancia presentó un problema que al parecer ya se le dio una solución relativamente fácil. Es común ver en algunos lugares avisos pegados a la pared con la silueta de una cámara impresa. Los carteles dan a conocer la presencia de cámaras y en ocasiones advierten con frases como "siéntase vigilado" y "evítese molestias". El contenido de muchos ha sido actualizado de forma que cumplan con el deber de información. Por su parte, la Guía de la SIC indica que estos deben "como mínimo, cumplir con el contenido de un aviso de privacidad"[109][110]. La idea es que la señalización sea el modo de obtener autorizaciones, amparados en la figura de las conductas inequívocas.

La autorización a través de conductas inequívocas es una figura llena de interpretaciones subjetivas y puede ser objeto de abusos. Para Remolina: "Esto generará incertidumbre jurídica y pérdida de tiempo en debates interpretativos."[111] El autor procederá entonces a perder el tiempo en debates, en alguna medida, interpretativos.

---

[109] Superintendencia de Industria y Comercio, *Protección de datos personales,* 7.

[110] Un aviso de privacidad es un medio por el cual el responsable da a conocer sobre la existencia de las políticas de tratamiento de datos y la forma de acceder a ellas (art. 14 del Decreto 1377 de 2013). Según el artículo 15 del mismo Decreto, el aviso de privacidad deberá contener: "1. Nombre o razón social y datos de contacto del responsable del tratamiento; 2. El Tratamiento al cual serán sometidos los datos y la finalidad del mismo; 3. Los derechos que le asisten al titular; 4. Los mecanismos dispuestos por el responsable para que el titular conozca la política de Tratamiento de la información y los cambios sustanciales que se produzcan en ella o en el Aviso de Privacidad correspondiente. En todos los casos, debe informar al Titular cómo acceder o consultar la política de Tratamiento de información. No obstante lo anterior, cuando se recolecten datos personales sensibles, el aviso de privacidad deberá señalar expresamente el carácter facultativo de la respuesta a las preguntas que versen sobre este tipo de datos."

[111] Nelson Angarita, *Tratamiento de datos personales*, 196.

El artículo 7 del Decreto 1377 estipula que un mecanismo para obtener la autorización con el lleno de sus requisitos es cuando se "manifieste […] mediante conductas inequívocas del titular que permitan concluir de forma razonable que otorgó la autorización. En ningún caso el silencio podrá asimilarse a una conducta inequívoca." Construir una discusión en torno a aquellas conductas que se pueda concluir o no de "forma razonable" consienten el tratamiento está de más. Incluso si se sustituyese 'razonable' por otros términos como prudente, justo, lógico, o sensato, en nada cambiaría el problema de fondo. Que una conducta o acción sea claramente afirmativa y así permita un tratamiento de datos lícito, será en muchos casos a discreción y conveniencia del responsable. Este método de obtener autorizaciones más allá de un mal necesario, parece ser una solución práctica.

Así se da la adopción masiva de esta figura para las actividades de videovigilancia. Obtener las autorizaciones por escrito o de forma oral es poco factible. La elección obvia es, como lo sugiere la Guía, los avisos distintivos o letreros mencionados anteriormente. Estos deben ser ubicados en lugares donde las cámaras todavía no capten imágenes y además deben ser visibles y legibles. En teoría, antes de acceder a las zonas vigiladas, las personas se toparían con dichos avisos y libremente decidirían si continuar o no. Algunos problemas que se pueden identificar rápidamente son el afán o el desinterés de las personas por leer este tipo de avisos, el analfabetismo o la población invidente. Esto resulta en una segunda dificultad y es que el Responsable puede no saber si el tratamiento es legítimo.

También parece dispendioso encontrar el respaldo de una autorización cuando un Titular la solicite por cualquier motivo[112]. ¿Cómo es el respaldo de una conducta inequívoca

[112] Literal b, artículo 8, Ley 1581 de 2012: "El titular de los datos personales tendrá los siguientes derechos: b) Solicitar prueba de la autorización otorgada al Responsable del Tratamiento salvo cuando expresamente se

como esta? Enseñarle al titular interesado las grabaciones hasta que se encuentre pasando por el área de los avisos supone darle acceso a los datos de todas las demás personas que pasaron por allí lo cual es inaceptable. En la nueva Guía sobre el uso de videocámaras para seguridad y otras finalidades de la Agencia Española de Protección de Datos (AEPD), sugieren garantizar el derecho de acceso "mediante escrito certificado en el que, con la mayor precisión posible y sin afectar a terceros, se especifiquen los datos que han sido objeto de tratamiento." Tal vez el mismo mecanismo pueda adoptarse para las pruebas de autorizaciones. Sin embargo, esto es imposible de cumplir cuando las imágenes se transmitan en tiempo real y no se almacenan.

Otros interrogantes surgen a partir de pensar cómo interactúa este mecanismo de autorización en el contexto de las cámaras con algunos temas abordados. Anticipándose a la rápida expansión de las nuevas tecnologías, piénsese por ejemplo en lo siguiente: ¿las cámaras con identificación biométrica pueden obtener autorizaciones través de estos avisos? Si el aviso cumple los parámetros de la Guía, es decir, su contenido es el de un aviso de privacidad, este mecanismo es inviable. Lo anterior porque cuando se van a recolectar datos sensibles, "el aviso de privacidad deberá señalar expresamente el carácter facultativo de la respuesta a las preguntas que versen sobre este tipo de datos."[113] En una cartilla o formulario es fácil añadir una casilla adicional con un pasaje que informe dicho carácter facultativo y el individuo pueda tomar una decisión sobre consentir el tratamiento de sus datos sensibles. Por otro lado, no se evidencia el carácter 'facultativo' del suministro de mis datos biométricos

exceptúe como requisito para el Tratamiento, de conformidad con lo previsto en el artículo 10 de la presente ley."

[113] Numeral 4, Artículo 15, Decreto 1377 de 2013.

mediante una conducta inequívoca como acceder a un sitio y leer un aviso por muy explicativo que sea.

El artículo 6 del Decreto en estudio, dispone que para obtener la autorización para el tratamiento de este tipo de datos se debe "Informar al titular de forma explícita y previa, además de los requisitos generales de la autorización para la recolección de cualquier tipo de dato personal, cuáles de los datos que serán objeto de Tratamiento son sensibles y la finalidad del Tratamiento, *así como obtener su consentimiento expreso."* [Itálicas nuestras] El último requerimiento parece redundante toda vez que la autorización en cualquier caso debe ser obtenida de manera expresa. Una posible interpretación es que para este tipo de datos, el consentimiento debe ser obtenido de manera aislada a la de los demás datos. Así el titular si podría disponer de sus datos libremente. De nuevo, de un letrero y el titular cruzando una línea imaginaria de acceso no se puede concluir que hubo un proceso volitivo en el que aquel aceptó la propuesta para que por un lado se traten sus datos generales y por el otro sus datos biométricos. Por lo que dichos avisos son insuficientes para satisfacer el principio de libertad en cuanto a datos sensibles.

Hay que anotar que en todo el RGPDP no se hace ninguna alusión a si los datos sensibles se encuentran excluidos o no de la excepción que le permite a entidades públicas y administrativas realizar actividades de tratamiento sin que medie autorización. Por lo que se asumirá que la excepción también cubre este tipo de datos, tanto en los eventos en que la entidad recoja los datos por su cuenta o encargue a un tercero de hacerlo. Lo anterior no solo se limita a la recolección si no a cualquier actividad de tratamiento como uso y almacenamiento. Así las cosas, los dos ejemplos de cámaras de identificación facial que se

han planteado – Transmilenio y estadios deportivos – las autoridades no tendrán que solicitar autorización de los titulares.

Caso diferente es el de personas naturales o jurídicas que aprovechen recursos técnicos y humanos para prestar los servicios a los que se refiere el Decreto 356 de 1994[114] y el Decreto 3222 de 2002[115]. Dentro de los servicios que ofrecen varias empresas de seguridad privada en sus portafolios están los de videovigilancia. Si bien el Estatuto de Vigilancia y Seguridad Privada contiene disposiciones en las que las bases de datos de dichas empresas pueden ser compartidas con la Fuerza Pública, esto no las exime de solicitar autorización a los titulares de los datos por su calidad de Responsables. Para estas empresas los carteles en porterías o ascensores de edificios con el contenido mínimo mencionado anteriormente es la vía hecha a la medida y avalada por el RGPDP.

En otro esfuerzo de la SIC para orientar a los responsables y encargados en el cumplimiento del RGPDP, la entidad difunde la cartilla "Formatos modelo para el cumplimiento de obligaciones establecidas en la Ley 1581 de 2012 y sus decretos reglamentarios". En el Anexo 2, "Modelo de autorización para el tratamiento de datos personales" se hace la siguiente advertencia: "Cada finalidad que usted incluya en este formato debe contar con un mecanismo que le permita al Titular seleccionar por separado si acepta o no que se efectúe ese tratamiento particular." Ninguna ley o decreto estipula la obligación de solicitar la autorización de cada finalidad por separado. Si esto fuese parte de la Ley 1581 desde el inicio seguro la Corte Constitucional lo aprobaría como una garantía al principio de libertad. Pero no es el caso. La Delegatura para la Protección de Datos Personales

[114] Por el cual se expide el Estatuto de Vigilancia y Seguridad Privada.
[115] Se reglamenta parcialmente el Estatuto de Vigilancia y Seguridad Privada y se crean las Redes de Apoyo y Solidaridad Ciudadana.

de la SIC, en ese entonces encabezada por María Claudia Caviedes Mejía, se pronunció al respecto en respuesta a una petición al respecto realizada por Nelson Remolina Angarita y el Observatorio Ciro Angarita Barón. En este, la entidad dice que si bien no hay norma que haga referencia específica a dicha obligación, de acuerdo la interpretación que le da al RGPDP, se infiere que no hay verdadera libertad si no se puede elegir sobre cada uno de las finalidades del tratamiento.[116] En el contenido restante de la respuesta, la SIC da respuestas amplias y un poco elusivas. Entre lo que dice (o no) y sirve rescatar, se aparta de referirse a la cartilla como una instrucción, prefiriendo el término "guía". También es extraño como parece minimizar y alejarse el asunto diciendo que *"debe tenerse en cuenta que dicha cartilla expone la interpretación legal de esta Entidad respecto de los temas a los que se refiere."* Como si no fuese un concepto de la autoridad encargada de la protección de datos personales firmada –si algo de valor simbólico aporta- por el Superintendente que estuvo liderando la elaboración e implementación del RGPDP por 6 años.

En todo caso no pienso que esa advertencia sea un capricho o un desliz de la SIC. En el Reglamento de la Unión Europea estipuló en sus consideraciones que: "Se presume que el consentimiento no se ha dado libremente cuando no permita autorizar por separado las distintas operaciones de tratamiento de datos personales pese a ser adecuado en el caso concreto […]"[117] Tal vez haya una conexión entre lo uno y lo otro. Para poder estar a la par con el desarrollo de los estándares europeos, la Superintendencia introdujo la advertencia. Al

[116] "[…] se concluye que si el modelo de autorización utilizado por un Responsable del Tratamiento da lugar a que el Titular deba consentir el tratamiento de sus datos para diversos fines, entre los cuales puede haber alguno o algunos que no le interesen o no quiera autorizar, sin darle la oportunidad de negarse a ello, la autorización obtenida no se traduce en una verdadera expresión de su voluntad, en la medida que no tiene libertad para decidir sobre cada uno de los tratamientos." [Respuesta a Petición del Sr. Nelson Remolina Angarita, *Superintendencia de Industria y Comercio*, 30 de junio del 2015, acceso el 17 de enero del 2019, https://habeasdatacolombia.uniandes.edu.co/wp-content/uploads/Concepto-SIC-cartilla-30V20181.pdf]

[117] Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, consideración (43)

igual que la Guía de videovigilancia, la cartilla no es el mecanismo idóneo para 'orientar' o más bien introducir esta obligación a los Responsables a la misma. En cualquier caso, si esa es la "interpretación legal" de la SIC sobre el asunto, ¿no es de esperar que la entidad comience a ejercer sus facultades sancionatorias en razón de dicha interpretación? Incluyendo ejemplo a quienes operan sistemas de videovigilancia por múltiples finalidades. Si lo anterior tendrá algún efecto real se sabrá si después de presentados los recursos de reposición o apelación respectivos, el Superintendente Delegado para la Protección de Datos sanciona a algún Responsable o Encargado en razón de ello.

Cerrando el tema de las autorizaciones. No creo que sea hermenéutica jurídica. El concepto se me escapa y seguro es entre impreciso y presuntuoso, ornamental casi. A falta de término correcto y molesto porque no quería hablar de ello hasta que la SIC lo puso sobre la mesa al intentar justificar lo de la autorización por finalidad, dejaré un par de ideas que rozan la 'verdadera' libertad de elegir suministrar mis datos. El desequilibrio en la relación entre los interesados en explotar los datos y los dueños de estos la disipa. Va más allá de mantener mi privacidad, es sobre acceder a servicios, bienes, espacios, relaciones, trabajo, etc. Denegar o revocar mi consentimiento sin sufrir algún tipo de perjuicio es muy difícil, incluso cuando no tiene una relación necesaria con aquello a lo que quiero acceder. Es casi sospechoso que alguien prefiera no entregar su información. ¿Cuántas cámaras capturan y registran mi pasar al día? ¿En cuántas de esas ocasiones me puedo detener a preguntarme si quiero o no que me filmen? Creo que habrá que pensar que hay un espectro de libertad 'razonable' en este sentido. Y moderar ese espectro es la función de la SIC. Con la tecnología que predomina hoy en las calles puede que la legislación actual sea en conjunto, satisfactoria. Pero no está lista para el auge de la identificación facial y la biometría sin comprometer la

autodeterminación informática de los ciudadanos. El desplazamiento de un lugar *A* al *B* queda registrado para ser consultado en otro tiempo y lugar y nadie preguntó si quería. Que ciertamente muchos beneficios ha traído la llamada edad de la información, pero faltará la tragedia correcta a la persona correcta para trazar sus límites. Frente a los innumerables usos que tiene la tecnología y las promesas que hace, Stefano Rodota se pregunta: "¿todo lo que es tecnológicamente posible es al mismo tiempo éticamente admisible, socialmente aceptable, jurídicamente legitimo?"[118]

Sobre la autorización y las videocámaras con fines como la seguridad y la vigilancia pienso que hay dos escenarios probables. El primero es que todo siga como está y las discusiones se queden en un plano hipotético donde un par de grupos de investigación curiosos sigan haciendo preguntas pero nada más. El segundo va en línea con lo que están haciendo ordenamientos europeos y requiere la modificación de algunas disposiciones del RGPDP. Se tendría que adoptar una nueva forma de legitimar el tratamiento de datos sin que medie autorización. En el Reglamento europeo, cuando "el tratamiento es necesario para el cumplimiento de una misión realizada en interés público […]"[119] el tratamiento es lícito sin solicitar consentimiento. Escudada en esta condición la AEPD sostuvo en la nueva guía que "puesto que la finalidad de la videovigilancia consiste en garantizar la seguridad de personas, bienes e instalaciones, el interés público legitima dicho tratamiento."[120] Así prescindieron de los avisos de las videocámaras.

[118] Stefano Rodota, "Democracia y protección de datos", en *Cuadernos de Derecho Público,* n° 19-20 (2003), 26.
[119] Literal e), Artículo 6 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo.
[120] Guía sobre el uso de videocámaras para seguridad y otras finalidades, *Agencia española de protección de datos,* p. 11*,* acceso el 17 de enero del 2019, https://www.aepd.es/media/guias/guia- videovigilancia.pdf

El viro de la Unión Europea al respecto tiene un impacto importante. Ellos son quienes han fijado la vara del tratamiento adecuado de datos personales y por eso es uno de los escenarios probables. Si la Unión considera que los sistemas de videovigilancia son de interés público y el tratamiento de datos que haga es legítimo, no veo por qué los países cuyo régimen de protección de datos es aprobado por la Unión – o buscan serlo – no puedan contemplarlo también. Si el ordenamiento colombiano fuese a adoptarlo, tendría que fortalecerse en: (i) el respeto por los principios y garantías los principios existentes; (ii) el desarrollo de una idea de intervención mínima y; (iii) la implementación de medidas como las evaluaciones y estudios de impacto, idoneidad, necesidad y proporcionalidad para poder instalar sistemas de videovigilancia. En conjunto esto resultaría mucho más efectivo a la hora de salvaguardar el *habeas data*. La función de los avisos sería para informar a los titulares de la existencia de los dispositivos de videovigilancia, su finalidad y proveerles información del Responsable o Encargado. Considero que la autodeterminación informática no se vería gravemente afectada por una razón ya expuesta. Son tantos los lugares de constante afluencia con videocámaras en la actualidad que la elección era más una ilusión. No obstante el atribuirle toda esta forma de vigilancia al interés público tiene conjeturas. Contrario a la seguridad pública con la seguridad privada solo se benefician unos pocos, y son muchos los que pueden ser afectados. Se confrontan el derecho de unos a proteger sus bienes y el de la protección de datos personales y autodeterminación informática de terceros. Los beneficiados por su parte puede que tengan el poder económico suficiente para que se acepte como un asunto de interés público.

Conclusiones

Los problemas y críticas hechas al RGPDP respecto a cómo regula las actividades de videovigilancia están solucionados por otros ordenamientos o por el mismo ordenamiento colombiano, después de todo este no es un tema novedoso dentro de la relación del Derecho con las nuevas tecnologías. Que la SIC no baje la guardia y mantenga al régimen relevante verificando que los Responsables realmente implementen programas para la gestión de datos personales es determinante. También hay que recordar el interés del Estado y el de algunos sectores económicos para alcanzar el nivel adecuado de protección de datos personales. Pero la efectividad del régimen también obedecerá en gran medida a la apropiación que el pueblo haga de sus derechos y de los mecanismos disponibles para defenderlos.

Sobre las observaciones hechas al ámbito de aplicación de la LEPD, solo queda decir que su redacción –parcialmente- en torno a las bases de datos como un requisito de aplicabilidad es desafortunada. La Corte Constitucional ya tenía unas bases desarrolladas en materia de *habeas data* y protección de datos personales en línea con las tendencias internacionales. Los datos como tal siempre habían sido el objeto de protección y cualquier tipo de tratamiento estaba sujeto a los principios recogidos. El tratamiento debió ser el único criterio tenido en cuenta para evaluar la aplicación del régimen. Sin forma de sustentarlo, una posible explicación es que el régimen fue estructurado en cierto sentido de arriba hacia abajo. Varias obligaciones que el RGPDP exige de algunos Responsables se cumplen a través del Registro Nacional de Base de Datos (RNBD). Esta plataforma facilita las funciones sancionatorias y de control y vigilancia de la SIC. También es una herramienta con la que cuentan los titulares de los datos para hacer valer sus derechos. Sin embargo la plataforma, como su nombre lo indica, opera en función de bases de datos. No se discutió el RNBD en

este trabajo porque es, en opinión del autor, un fracaso condenado a desaparecer. En España una plataforma similar llamada el Registro General de Protección de Datos creada por la Ley Orgánica 15/1999 fue sustituida por un registro de actividades de tratamiento que deberá llevar cada Responsable[121]. Para dicho registro las bases de datos son irrelevantes por lo que las cámaras que capturan imágenes en tiempo real también deberán llevar su registro. Tal vez el mismo futuro le depare al RNBD. Los decretos que reducen el espectro de Responsables obligados registrar sus bases en la plataforma, el último siendo el Decreto 090 de 2018, puede ser indicio de esto. A propósito de estos, usar los activos del Responsable como el criterio para estar sujeto o no a la obligación de registro es una clara muestra del desconocimiento del legislador el cual no tuvo en cuenta que es probable que este tipo de activos inmateriales no hayan sido valorados por las empresas que los poseen.

De los sistemas de videovigilancia y otras formas de vigilancia que se valen de datos biométricos hay que recalcar que hay una prohibición expresa en la ley sobre condicionar actividades al suministro de datos sensibles. Tal vez el superintendente delegado actual abordará el tema del elefante en la habitación eventualmente. Desde la posición de que no es deseable que estas tecnologías queden a la deriva y operen en sí mismas como ley, rehusarse a consentir el uso de este tipo de datos cuando una actividad o servicio es condicionada al suministro de los mismos es lo justo. Mientras no se demuestre la efectividad de los sistemas de videovigilancia biométrica y que son menos lesivos para los derechos de los titulares que otros métodos de seguridad, deben ser rechazados.

El Estado parece que puede recoger datos sensibles sin la autorización de sus titulares. Los estudios de impacto y proporcionalidad contemplados en el Reglamento de la Unión

[121]Artículo 30 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo.

Europea deberían adoptarse en el ordenamiento colombiano como el contrapeso de este poder en cabeza del Estado. De esta forma la implementación de sistemas de vigilancia tan agresivos obedecería a estadísticas, información policial y la naturaleza del espacio (público, privado de uso público y privado). En este sentido la Agencia Española de Protección de Datos en su nueva guía de videovigilancia dispuso supuestos puntuales en los que el tratamiento de imágenes con fines de seguridad, construyendo espacios regulados no de forma abstracta sino concreta como en los casos de lugares de infraestructura crítica, joyerías, entidades financieras y otras.

En el asunto de la autorización y la legitimación del tratamiento, la AEPD ahora argumenta que "puesto que la finalidad de la videovigilancia consiste en garantizar la seguridad de personas, bienes e instalaciones, el interés público legitima dicho tratamiento."[122] La adopción 'solución' por parte del ordenamiento colombiano sería viable en la medida en que haya mucha confianza en las instituciones y una fuerte presencia de la SIC. Por ejemplo se necesitarían compromisos como abandonar la retroalimentación y entre medios de comunicación y los operadores de los sistemas de videovigilancia a menos de que haya una orden judicial u otra autorización de las autoridades de por medio. Los avisos pueden continuar cumpliendo una función informativa sobre el Responsable, las finalidades puntuales y los canales que este habilita para atender a los titulares. También hay personas desarrollando formas de crear, con tecnología existente, sistemas de videovigilancia más seguros. Un grupo del departamento de ingeniería informática y matemáticas de la

[122] Guía sobre el uso de videocámaras para seguridad y otras finalidades, *Agencia española de protección de datos,* p. 6*,* acceso el 17 de enero del 2019, https://www.aepd.es/media/guias/guia- videovigilancia.pdf

Universitat Rovira i Virgili recogió varias formas de proteger las imágenes recogidas por estos sistemas como el encriptamiento de datos[123].

Todavía quedan cuestiones sociales que quedan por fuera del espectro del RGPDP y la regulación de la videovigilancia. El caso expuesto de las videovigilancia biométrica en los estadios del país es un reflejo de la siguiente reflexión. Hay que señalar la forma en que la Comisión enfocó la atención del sistema en las tribunas populares, a las cuales cataloga como un grupo potencialmente disruptivo para el ambiente en los estadios o de 'desadaptados sociales'. La segregación y prejuicios derivados de este tipo de decisiones han sido naturalizados por el discurso de la seguridad pública y por el proverbio bíblico de 'el que nada debe, nada teme'. En función del imaginario estereotipado que los aparatos de poder – la Comisión- tienen sobre las tribunas populares, las personas que asisten a estas locaciones son sometidas a un proceso de estigmatización social soportado únicamente por la expectativa de resultados, es decir, la efectividad. A través de la vigilancia que propone la carnetización y las videocámaras, los comportamientos que se consideran antisociales son despojados de su contexto social, y las causas que provocan fenómenos como las "barras bravas" pasan a otro plano. Etiquetar, clasificar y tipificar un grupo social de acuerdo a la tribuna que asisten y a la información exagerada que la Comisión pide considerar, es implementar de manera abierta una política en la que un colectivo es sometido a un proceso de escrutinio marcado por perjuicios que derivan en exclusión Además, la priorización de estas tribunas afecta el ejercicio de los derechos de estos aficionados, toda vez que mina la capacidad de las barras de hacerles frente a esas lógicas de clasificación social. Los esfuerzos

[123] Rashwan, Hatem, Agusti Solanas, Domènec Puig, and Antoni Martínez-Ballesté. 2016. "Understanding Trust in Privacy-Aware Video Surveillance Systems." *International Journal of Information Security* 15 (3): 225–34

por parte de algunas barras organizadas de solucionar los problemas de desorden y mal comportamiento desde su autonomía y sus dinámicas pierden legitimidad cuando se les imponen sistemas de vigilancia tan desproporcionados e invasivos. La instrumentalidad y la efectividad no pueden desplazar la discusión ética y ser el único criterio que gobierna las políticas de vigilancia. Sin embargo, desde la promulgación de la Ley 1270 de 2009 a hoy este cuadro no es el mismo. Lo primero que cambió es que para ese entonces no existía el RGPDP ni una autoridad de protección de datos personales. Lo segundo es que en 2014 a través del Ministerio de Interior y la Comisión se adoptaron el Plan Decenal de Seguridad, Comodidad y Convivencia en el Fútbol que moderó el discurso hacia las barras y le apuesta a estrategias con mayor participación de las comunidades, los actores del fútbol y expertos[124].

El RGPDP debe continuar evolucionando y requerirá de más herramientas para hacerle frente al poder informático. Es un avance importante toda vez que el pueblo ya no es el único que está siendo monitoreada. Aquellos que están detrás de las cámaras ahora tienen también una forma de gobierno. Que Colombia llegue a ser reconocida como un país con niveles adecuados de protección de datos es un incentivo importante para que el Estado le siga apostando a su desarrollo. Sin embargo no se puede olvidar que el *habeas data* no es solo un derecho, también es una herramienta de control que tienen las personas sobre sus datos personales y su protección depende en gran medida en el valor que estos le concedan.

[124] Alejandro Villanueva, Alirio Amaya y Nelson Rodríguez, autores del libro *Hasta que el cuerpo aguante* (2011) sobre el fenómeno del barrismo fueron invitados a hacer parte del comité de redacción del Plan.