El uso estatal de las tecnologías biométricas de vigilancia afectación de los derechos a la privacidad, a la intimidad y a la propia imagen

Por:

Jovany Aleces Pabón Restrepo

Universidad Autónoma Latinoamericana

Facultad de Derecho

Medellín

Abril, 2020

El uso estatal de las tecnologías biométricas de vigilancia afectación de los derechos a la privacidad, a la intimidad y a la propia imagen.

Por:

Jovany Aleces Pabón Restrepo

Monografía como opción para optar al título de abogado

Asesor

Gillante Hernández Ríos

Universidad Autónoma Latinoamericana

Facultad de Derecho

Medellín

Abril, 2020

Tabla de contenido

Resumen

Los adelantos en la ciencia informática, de la inteligencia artificial, han propuesto escenarios antes insospechados para la vulneración de garantías y derechos fundamentales, allí la tecnología biométrica contribuye en la posibilidad de identificación, contraste, verificación o reserva de los datos personales. Los datos atienden a diferentes clasificaciones en los ordenamientos jurídicos, pueden ser públicos, reservados, privados, pero de manera específica atienden a la denominación de sensibles, entendidos como la clase de información que requiere de un especial tratamiento por parte de las personas obligadas al demandar circunstancias preferentes para su acceso como es de suerte exclusiva en casi todas las legislaciones el consentimiento otorgado por el titular. Si se pierde de vista este contexto logra comprometerse la observancia de garantías fundamentales como son la privacidad, la intimidad y la propia imagen, conceptos o derechos que son interpretados de manera diferente en cada codificación.

La reglamentación es escasa sobre el tema o avanza a menor ritmo que el desarrollo de las tecnologías. Situación que es aprovechada por los Estados o sus agencias para realizar monitoreo y vigilancia sobre la sociedad en general, sin el respeto de los pocos instrumentos jurídicos adecuados para el tratamiento de datos sensibles. Las técnicas de identificación biométricas han facilitado esta labor, debido a su probada eficacia y los bajos costos de implementación, sumado al auge comercial de tecnologías como el reconocimiento facial que se ha integrado con agencias de aplicación de la ley en la certeza de que a través de estas se puede ver, oír, grabar, contrastar, verificar, transmitir en vivo, sin requerir el consentimiento del titular. Violentando su privacidad e intimidad, además de propiciar situaciones que reprimen entre otras el libre desarrollo de la personalidad, generan discriminación, desigualdades, al vulnerar de forma palmaria el concepto de estas garantías y derechos fundamentales.

Palabras clave: Datos sensibles, privacidad, intimidad, derecho a la propia imagen, tecnologías biométricas, reconocimiento facial.

Abstract

Advances in computer science, artificial intelligence have proposed previously unsuspected scenarios for the violation of fundamental rights and guarantees, biometric technology means the possibility of identification, contrast, verification or reservation of personal data. The data are classified in different legal systems, they may be public, reserved, private, but they specifically address the denomination of sensitive, understood as the kind that require special treatment by the persons obliged to demand different circumstances for access as can be of exclusive luck in almost all the legislations the consent granted by the holder. Losing sight of these contexts may compromise the observance of fundamental guarantees such as privacy, intimacy, right of publicity, concepts or rights that are interpreted differently in each codification.

Legislation on the subject is weak or is progressing at a slower pace than the development of technologies. This situation is used by States or their agencies to monitor society in general, without observing the few legal instruments available for the processing of sensitive data. Biometric identification techniques have facilitated this work because of their proven effectiveness and low implementation costs. Coupled with the commercial boom of technologies such as facial recognition that has been integrated with law enforcement agencies, in the certainty that through it you can see, hear, record, contrast, verify, broadcast live, without requiring the consent of the owner, violating their privacy and intimacy, encouraging situations that repress, among others, the free development of their personality, generate discrimination, inequalities, and blatantly violate the concept of fundamental rights and guarantees.

Keywords: Sensitive data, privacy, intimacy, right to publicy, biometric technologies, facial recognition.

1. Introducción

Esta monografía de grado pretende identificar como se concreta la vulneración y el tipo de lesión que se realiza en los derechos fundamentales a la privacidad, a la intimidad y a la propia imagen, con el tratamiento por parte del Estado de las categorías especiales de datos a través de los sistemas de vigilancia masiva con tecnologías biométricas. Logro que se proyecta alcanzar mediante una búsqueda, recopilación y procesamiento de la información recolectada en fuentes primarias referidas al tema en la legislación, la jurisprudencia, la doctrina, de tres ordenamientos jurídicos específicos a saber; Colombia, la Comunidad Europea con punto de referencia en España por la semejanza idiomática, además los Estados Unidos por su denominación de Estado tecnológico promotor de tecnologías biométricas. Para dar consistencia a los marcos conceptual y teórico se abordarán las anteriores fuentes complementadas con otras secundarias e insumos obtenidos en artículos de revista, periodísticos, informes científicos, blogs de opinión, varios.

En este entendido e inicialmente con el objeto de identificar el alcance de dato sensible se indagará para hacer claridad del concepto, realizando en un primer capítulo un contraste de lo dispuesto para su definición en los diferentes instrumentos normativos de estas legislaciones. Consecuentemente se realizará, en un segundo capítulo, una definición jurisprudencial, legal, así mismo de doctrina de los derechos a la privacidad, a la intimidad y a la propia imagen, en los ordenamientos jurídicos señalados, abordando los conceptos mediante su consideración en providencias, leyes, estudios que sobre estos derechos se han pronunciado. Teniendo para este propósito como estrategia, identificar el punto donde se ha fundado el concepto y los desarrollos posteriores que han contribuido a consolidarlo. Otro capítulo desarrollara fugazmente la técnica de recopilación o contraste de datos denominada biometría, por lo cual se realiza a través de un atajo de rastreo una abreviada definición de su esencia, sus usos modernos, marco legal que la

soporta como instrumento de recolección, tratamiento y almacenamiento de datos, con su postrer aplicación en virtud del principio de interés general, como herramienta en la seguridad de los denominados Estados tecnológicos.

Se planteara así en un último capítulo la tensión generada entre las diferentes tácticas o estrategias a través del uso de tecnologías biométricas de seguridad implementadas por el Estado o sus agencias, con el posible tratamiento de datos sensibles y su convergencia en el establecimiento de modelos de vigilancia tipo panóptico, asimismo la aparición de políticas de control generalizadas que entran en lid con las garantías de protección debidas a los derechos fundamentales. Se analizarán en tal sentido las interceptaciones o escuchas telefónicas en Colombia por ser hecho notorio. Al lado de ello en los U.S se estudiará la tecnología biométrica de reconocimiento facial para la vigilancia o monitoreo, por el notable incremento de uso comercial al mismo tiempo que se entrecruzan datos con las agencias de aplicación de la ley o del sector público. Finalmente se darán las conclusiones como resultado de la investigación.

2. Pregunta

¿Cómo se afectan los derechos a la privacidad, a la intimidad y a la propia imagen, mediante el uso de tecnologías biométricas de vigilancia para la seguridad estatal?

3. Objetivos

3.1 Objetivo General

Identificar en el Derecho comparado el tipo de lesión que realizan los Estados a las garantías fundamentales a la privacidad, a la intimidad y a la propia imagen, a través del uso de tecnologías biométricas de vigilancia para su seguridad.

3.2 Objetivos Específicos

- Indagar el origen del concepto de dato sensible y cómo se ha configurado en la legislación e instrumentos de los ordenamientos jurídicos señalados.
- Analizar los conceptos privacidad, intimidad, derecho a la propia imagen.
- Rastrear el concepto de biometría, su evolución a tecnología biométrica, su uso como estrategia de control para los Estados.
- Constatar la lesión a los derechos fundamentales relacionados.

4. Marco teórico

La necesidad de identificarse o verificar identidades, es inherente a la conformación de la sociedad en el propósito de salvaguardar instancias como; la propiedad, la familia, reconocer derechos, asignar cargas, penas. La biometría históricamente ha sido usada tanto para la seguridad como para la salud. Así en la sumeria antigua los comerciantes ya se identificaban con su huella dactilar dejada como marca en una tabla de arcilla para acceder a las mercancías otorgadas en depósito. (Borja, 2019)

En las sociedades expulsoras de Roma y Grecia se mutilaba a los transgresores de la ley para identificarlos con la intención de exiliarlos al margen de la población. Otras prácticas marcarias se extendieron a lo largo del devenir desde la cultura clásica, en un intento de control poblacional y como cimiente proyectual de los modernos sistemas carcelarios.

Foucault en la sociedad punitiva plantea que el marcar, herir, mutilar, poner signos tatuados "G", son entre otras, las formas que el poder tiene para apropiarse del cuerpo en la denominada sociedad de marcación a fines de la edad media (Foucault. 1972-1973). En el surgimiento del sistema carcelario se idearon igualmente procedimientos más humanos para identificar y controlar a los individuos, muchos que en ciertas ocasiones partían de una falsa premisa moral o prejuicio en el físico o apariencia de las personas. Génesis para esta clase de identificación, fue la implementada por Aristóteles en siglo III A.C con su Physiognomonia (Altuna, 2011, p. 23). Allí insiste en la dependencia latente del cuerpo-alma, su inminente correlación con el estado anímico o los estados psíquicos. En el entendido de que determinada forma del rostro o del cuerpo equivale a una clase de carácter o alma así mismo esquematizado. Esta propuesta marco el rumbo de la biometría hasta muy avanzado el siglo XIX, para ser

reemplazada poco a poco por trabajos con más base científica, como la frenología de Franz Joseph Gall, médico austriaco que defendió la idea de que el cerebro da la forma al cráneo y que las facultades mentales se ubican en zonas específicas localizadas en este (Arias, 2018).

Otras teorías como el mesmerismo, la de los humores o el vitalismo, si bien hoy en rigor científico son absurdas, en su tiempo representaron certezas médicas, mismas que evolucionaron a estados superiores a principios del siglo XX con el autor italiano Cesare Lombroso, galeno y antropólogo del positivismo jurídico célebre por su hombre delincuente y su teoría del criminal nato, elementos o posturas que hoy pueden considerarse uno de los basamentos para la Criminología moderna y las prisiones (Da Re y Maceri,2007). Pero la biometría adquiere otro rumbo, a fines del siglo XVIII hace incursión la mirada de quien ostenta el poder, mirada que vigila y que mata. El modelo del panóptico, propuesto por el jurista inglés Jeremy Bentham, funciono como una institución de control, siendo en sus inicios implementado a modo de piloto para las prisiones combinando elementos tales como un método especial de vigilancia, enmarcado en una construcción arquitectónica de tipo circular con una torre central que observa la periferia. (Bentham, 1979)

Foucault estudia esta propuesta transformándola en panoptismo, porque aunó un control más diferenciado y exclusivo sobre los individuos catalogándolos; en sano-no sano, normal-anormal, razonable-no razonable, productivo-ocioso. Para finalmente desbordar como patrón el campo inicial planteado de las prisiones y completar su periplo de implementación en otros ámbitos a través de prácticas de corrección en instituciones de salubridad, seguridad, educación, en factorías o talleres, en el control del tiempo y del ocio, todo esto al servicio de una tecnología política (Foucault, 2016). Así el efecto de la biometría en el panóptismo es conducir de manera cauta a los individuos y a la sociedad en su conjunto, a un estado de vigilancia que desplace

mansamente los métodos de marcación que requieren coacción física directa, de suerte que ya no son necesarios medios de fuerza franca para obligar al condenado a la buena conducta, al loco a la tranquilidad, al obrero al trabajo, al estudiante a su aplicación. Foucault (2015).

Desde entonces el modelo de Bentham (1979) ha sido según sus propias conclusiones la cimiente para la cesión de la libertad de la sociedad además de los individuos, con la grave consecuencia de inducir en la certeza de que tal procedimiento florece para ser aceptado de forma voluntaria: “es la trama para el menoscabo de la libertad y de la privacidad mediante un proceder tenue que hace que se acepte sin reflexiones por la comunidad en su propio detrimento.” (pág. 84 y ss.)

La Libertad es un concepto demasiado amplio en tanto abarca desde las concepciones republicanas atravesando las luchas del liberalismo, pero puede concretarse finalmente en dos aspectos; la Libertad moral del individuo correspondiente al campo interno dominado por la razón y la autonomía, el segundo aspecto corresponde a la Libertad social o política, entendida como un espacio que requiere de la acción comunitaria al lado del ejercicio de la política (Gaviria, 2013)

La propiedad deviene sinónimo de la libertad en sus múltiples acepciones; de expresión, de prensa, de información, de locomoción, de culto, de enseñanza, de aprendizaje, de asociación. La privacidad o la intimidad garantizan el derecho a ser dejado solo en las decisiones que un individuo asuma de la libertad para sus usos moral y político. La intrusión del Estado y de los medios de comunicación es un freno a las libertades individuales. La mirada constante del Estado con sus sistemas de control puede constituir un obstáculo al desarrollo de la personalidad y a la felicidad de los individuos. También inciden los desarrollos de la tecnología que a manera de máquinas auscultan, miran, datean el cuerpo. (Warren, 1890). La privacidad tiene un

desarrollo jurisprudencial proveniente de la doctrina en el derecho anglosajón, el progreso exponencial de los medios de comunicación ha jugado un papel determinante en la vulneración a los derechos a la privacidad, a la intimidad, a la propia imagen. Por esto el perfeccionamiento constitucional del derecho a la privacidad o a la intimidad, está indisolublemente ligado a la consolidación del derecho a la información.

La Conferencia Nórdica sobre DDHH de Estocolmo en 1967. Señala que el derecho del individuo a vivir su propia vida está protegido de injerencias arbitrarias en su esfera privada y familiar, esto en consideración de que los avances en tecnología generan invasiones a la intimidad. (Juristas, 1967)

En la declaración de la sociedad civil Española, se advierte sobre la no consideración de las nuevas prácticas de vigilancia y los procedimientos con identificadores biométricos, resalta la obtención de bases de datos para entrecruzarlas en el sector público y privado con los consecuentes riesgos de vulneración a grupos específicos, más el deterioro en la protección de derechos y libertades (Conferencia Internacional, 2009)

Los que además gozan de amparo especial en el ámbito de la red, particularmente la libertad de expresión, que se hace extensible sin consideración de fronteras, como del procedimiento que se elija. (Consejo de Derechos Humanos, 2019)

> De otro lado la Intimidad es definida como la parte de la vida de una persona que no puede ser observada desde el exterior, porque solo concierne y afecta sólo a esta. Se incluye dentro del ámbito privado de un individuo a su familia, a su gremio de trabajo y cualquier información que se refiera a sus datos personales, relaciones, salud, correo, comunicaciones electrónicas privadas. (Sentencia T-364/18).

Los datos en las personas atienden a diversas clasificaciones, pero definitivamente están consignados en el rotulo de públicos y privados. Lo privado es lo que se opone a lo público, este último es toda información en cabeza de un sujeto obligado. Concretamente el derecho a la intimidad se concibe como un derecho humano fundamental que tiene sustrato en el respeto a la dignidad, en virtud de la facultad de las personas físicas de negar el conocimiento de su vida privada. Este tipo de datos que solo conciernen a las personas están clasificados como datos sensibles o categoría especial de datos.

La sentencia 94 de 1998, dispone la garantía a toda persona física para la protección de sus datos personales, y la consecuente prohibición para que sin su consentimiento se divulguen datos que ocasionen perjuicios y vulneraciones a los derechos que le son inherentes como son la intimidad, dignidad, honra. (Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales). Sin embargo, el derecho a la protección de datos y a la intimidad se concibe como no absoluto por estar dispuesto en función a su interés social y en armonía con otros derechos fundamentales. Los datos sensibles tienen un antecedente en el contexto europeo al residir en la directiva 95/46/CE, en donde son catalogados con el sello de categoría especial de datos, se incluyen en este instrumento por primera vez los datos biométricos y genéticos. En Colombia están consignados en la ley 1581 de 2012 artículo 5, en armonía de lo considerado en la Directiva. Finalmente, la última novedad en la protección de datos es dispuesta en el instrumento (UE) 2016/679 del Parlamento europeo y del Consejo, del 27 de abril de 2016, léase; Reglamento General de Protección de Datos. (Reglamento (UE) 2016/679) El reglamento proyecta ser una barrera de contención a los riesgos que conlleva el acceso el uso de la información por la inteligencia artificial, también unifica la polisemia

legislativa de la (UE) bajo un solo concepto, e irradia otros ordenamientos jurídicos como Brasil, Japón y en los U.S con la CCPA.

Como consideración teórica final se conoce que la IA y los avances tecnológicos permiten la captación indiscriminada de datos aun sin necesitar contacto o requerir consentimiento, muchos Estados aprovechan la coyuntura histórica y los vacíos legislativos para utilizar este tipo de técnicas en la comisión de delitos unos, para tal propósito se confabulan con agencias, comercio, compañías privadas. Pero todos finalmente generan polémicas por la consabida desnaturalización del hombre en el entendido de que se percibe una victoria de la IA sobre las personas y las comunidades. El hombre genérico es abordado por el poder a través de las máquinas y al llegar a este punto su mirada se hace más penetrante, se pierde en humanidad lo que se gana en cifras, números, logaritmos, datos. Deleuze (1999). En la actualidad estos desarrollos de la Inteligencia artificial han cercado a las comunidades e individuos en cómodos marcos de registro de sus datos personales para el comercio, los Estados y sus agencias. Se asiste al evento de la entrega voluntaria de la libertad, por no ser necesaria la mediación externa de realización de tareas físicas de coacción.

En el panóptico de Bentham se precisaban de barrotes o violencia para el control, para la seguridad e higienización, actividades todas que caben enmarcadas teóricamente en la explicación moderna y foucaultiana de biopoliticas. Hoy se migra sin retorno a una vigilancia tipo panóptico digital. Ya no es solo el Estado y sus agencias o facebook, microsoft, amazon.

Al presente cada persona e individuo se observan mutuamente, observamos y somos observados, es más nos observan cosas que nos rodean y usamos en la cotidianidad. Ya no es necesario un control externo como poder activo al que uno puede oponerse, en la actualidad el control tiene perfección por que deviene de la explotación que cada individuo realiza sobre si, la

biometría permite el análisis de nuestro comportamiento como individuos o comunidad, nos examina internamente, físicamente, conductualmente exponiendo nuestro inconsciente individual y colectivo, prediciendo conductas, detectando falencias, enfermedades, factores que son utilizados para ejercer un control total y sin barreras que puede ser traducido en una nueva teoría que bien sabe ser llamada psicopolitica (Byung-Chul Han, 2014)

5. Metodología

Se ha tenido como base para elaborar este trabajo de investigación, el libro de Jaime Giraldo Ángel "Metodología y técnica de la investigación jurídica", capitulo 5: "La monografía jurídica." (Ángel, 2012)

5.1 Tipo de estudio

En primer término, logra decirse con Sabino (Sabino, 1996), que alcanza a ser de tipo exploratorio por referirse a una cuestión poco abordada sobre la que es difícil enunciar hipótesis posibles para su demostración, debido esencialmente a la escasa legislación, al lenguaje técnico, las barreras idiomáticas y la poca disponibilidad de información. También es una monografía o investigación de tipo jurídico sociológica, al requerir que la respuesta para el tema de investigación se realice y se proyecte a corto plazo, porque debe ser buscada en una acorde interpretación de las fuentes formales del derecho y en la observación de la realidad que circunda. Para los abogados la interpretación del derecho es una invariable actividad de hacer, que consiste en traducir no solo en el plano legal, sí no que también se sitúa en campos más amplios y en otras esferas de conocimiento así la interpretación del texto legal es una narración

que sirve de plano de inmanencia para interpretar otra narración; la narración de los hechos, el caso. (Garces, 2010)

Consecuentemente es válido afirmar que este trabajo es de sentido interdisciplinar, disciplinar y en ocasiones contradisciplinar, esto último porque muchas afectaciones a ciertos derechos denominados fundamentales pueden estar explicadas en planos diferentes a los abordados por el derecho sustancial, por lo cual otros análisis se hacen necesarios para poder explicar.

5.2 Método

Inductivo y en Derecho comparado; lo primero porque se trata de la recolección de datos con observaciones sobre un tema específico y de su posterior estudio para la formulación de las conclusiones e hipótesis que ayuden a explicar la generalidad del problema. Lo segundo por ser el derecho comparado una escuela de la verdad (Zweigert, 2002) que intensifica la oferta de soluciones a la vulneración de los derechos fundamentales a través de la vigilancia con tecnologías biométricas.

5.3 Enfoque

Es un estudio con enfoque cualitativo por realizar preferiblemente equivalencias o analogías directas del contenido de sentencias, jurisprudencia, doctrina y otras fuentes en el derecho comparado que coadyuvan a constatar la actividad de los Estados en la lesión a las garantías fundamentales relacionadas. De otro lado, es también una investigación de tipo valorativo descriptivo con un enfoque cualitativo, por tratar de identificar en el derecho comparado propuestas que acerquen en la búsqueda de resultados.

5.4 Diseño

A partir de una hipótesis lógica realizar actividades exploratorias con lecturas reflexivas al mismo tiempo críticas en el derecho comparado, pensado o encaminado a establecer una claridad conceptual para concretar así un amplio conocimiento sobre el tema en todas sus partes y poder constituir sus relaciones. Labor que debe conducir necesariamente a la confección de un escrito como balance del objetivo buscado que es dar respuesta al tipo de vulneración o lesión a derechos fundamentales realizada por los Estados a través de las tecnologías biométricas.

5.5 Técnicas e instrumentos

La revisión documental y analogía directa en fuentes primarias que aborden el hecho como son sentencias, jurisprudencia de las cortes constitucionales, doctrina, informes, correspondencia. Además, la observación de los hechos reflejados en la implementación practica de sistemas de vigilancia o identificación con tecnología biométrica.

Fuentes secundarias como revistas, informes periodísticos, páginas web, pero teniendo en cuenta la veracidad y el rigor critico que avale al medio.

Como técnica se utilizará el análisis de la información y se elaboraran fichas que sinteticen la búsqueda en material impreso. También como herramienta de trabajo se recabará en internet por la gran facilidad y disponibilidad de información en este medio.

6. Formulación del Problema

En derecho comparado se tienen instrumentos y mecanismos que salvaguardan la privacidad, intimidad e imagen de las personas denominadas físicas. La inteligencia artificial y las tecnologías biométricas son áreas de conocimiento novedosas que despliegan oportunidades de progreso, comodidad y mejora para la humanidad, pero paralelamente son realidades contrarias a las libertades y derechos civiles especialmente para su vulneración cuando son implementadas sin un marco legal omitiendo la protección a las garantías fundamentales. En tal sentido los Estados buscan siempre la adecuación de métodos que les resulten eficientes y económicos para el control de las comunidades e individuos, proceso en el que no pocas veces se extralimitan en sus funciones al realizar un tratamiento ilegal e indebido de datos. Es entonces que con ocasión de este trabajo y monografía de investigación se realizara la búsqueda para responder:

¿Cómo se afectan los derechos a la privacidad, a la intimidad y a la propia imagen, mediante el uso de tecnologías biométricas para la vigilancia y seguridad estatal?

7. **Justificación**

Esta monografía de investigación resulta útil como instrumento exploratorio por la novedad, actualidad, además del poco conocimiento del efecto que esta realidad tiene que sobre las personas. Pedro Nikken, expone que los derechos humanos son inherentes a estas, consecuencia de esa inherencia devienen la universalidad e irreversibilidad de los mismos. El derecho ha librado batallas para enunciar o afirmar ciertas garantías fundamentales que hoy las tecnologías y el auge de la inteligencia artificial además de su mal manejo por los Estados puede suprimir. (Nikken., 1994). Los sistemas biométricos son también considerados en condición de

universalidad por extraer los rasgos físicos a manera de datos que están presentes en todo individuo. Tal es que un programa de IA o una tecnología biométrica puede conocer todo sobre estos eventos que consistiría en una fuerte intromisión en la intimidad y un duro golpe a la privacidad y al derecho a la propia imagen tal como se han logrado consolidar hasta hoy.

El avance exponencial de estas ciencias especialmente en el último lustro en los denominados Estados Tecnológicos con los Estados Unidos y China a la cabeza, proponen escenarios escalofriantes en una sociedad de control. Con el agravante de que ya no se despliega un control físico de coacción sobre las personas como el propuesto en el modelo de panóptico de Bentham, si no que hoy la sociedad denominada liquida posibilita a través de los medios de comunicación, el que sean los propios individuos quienes voluntariamente expongan su imagen, su perfil, cediendo de esta forma su libertad a un Estado que parece omnipotente por la falta de resistencia. (Ortiz, 2019) Pero el uso de estas tecnologías no se limita al sector público también el comercial y privado se han alzado en complicidad con las agencias del Estado resaltando aún más el problema al diseñar, patentar además de producir software y hardware que captan de manera intrusiva toda clase de datos. Estas tecnologías llegaron posiblemente para quedarse, el reto social, de los legisladores, de la política, consiste en hallar formas de convivencia que limiten su uso y al mismo tiempo no tracen cortes sesgados que confinen la humana naturaleza vulnerando derechos fundamentales.

CAPITULO 1

7. Definición de datos sensibles o categoría especial de datos

8.1 Origen y antecedentes del concepto de dato sensible

Datos sensibles

Según la Real academia de la lengua, sensible es en el idioma Castellano "lo que tiene la calidad de delicado, susceptible, blando. O definido como adjetivo; el que por su naturaleza debe ser tratado con especial cuidado" RAE. Las diferentes clasificaciones de los datos, se basan en el derecho que pueden tener las personas físicas o jurídicas para proteger su integridad, también la calidad de privacidad o reserva del documento que se requiere para ser tratado o almacenado y en mayor grado al tipo de riesgo u afectación que conlleva a su titular. En este apartado se rastrea y analiza el término dato sensible en tres situaciones puntuales a saber: el ámbito colombiano, el europeo, léase (UE) y los Estados Unidos, en adelante U.S.

8.2 Colombia

La ley 1712 de 2014 tiene como objeto regular el derecho de acceso a la información, así como los procedimientos, garantías y excepciones para este propósito. Esta Ley se encarga de preceptuar acerca de la información catalogada como Publica, o toda clase de información que un sujeto obligado pueda generar, obtener o controlar en su condición, delimitándola en dos vertientes como son; la información pública reservada y la denominada información pública clasificada. La información pública reservada está en cabeza de los llamados sujetos obligados, en donde se incluyen por su ámbito de aplicación todas las esferas del sector público, en todos

sus niveles y calidades ya que atañen necesariamente al ejercicio de la función pública a tenor de lo estipulado en el artículo 5 de la referida Ley.

El acceso a la información pública catalogada como reservada puede ser en este contexto, objeto de negativa si se acomoda a las excepciones de entrega o acceso del artículo 19 literal a, que resalta el tipo de información relacionada con los asuntos de defensa y seguridad nacional. La información pública clasificada, en tanto es definida como; "Aquella información que estando en poder o custodia de un sujeto obligado en calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado" (Ley 1712, 2014). Aquí la negativa del obligado a suministrar este tipo de información o datos puede estar justificada en eventos donde se lesione la vida, la intimidad, la seguridad, la salud de las personas, así como de las empresas industriales y comerciales del Estado, también las sociedades de economía mixta en el evento de estar exentas de aportarlos cuando se trate de información relacionada con sus proyectos de inversión. (Ley 1474 de 2011)

La información pública catalogada como clasificada, adquiere así dos nuevas vertientes hacia la cual fluye en calidad de datos impersonales y datos personales, contenidos los primeros en el artículo 3 de la ley 1266 de 2008, subdivididos a su vez en privados de igual modo que en semiprivados según rotulación en el susodicho artículo numerales g y h. En tal sentido el dato impersonal semiprivado se destaca por ser un tipo de dato que no tiene una naturaleza íntima además por ser de interés solo para su titular, en tanto el dato publico clasificado como de carácter impersonal privado, es enunciado como aquel dato que por su naturaleza intima o sensible solo es relevante para el titular o interesado. Consecuente con lo anterior los datos de tipo personal están reglamentados en la ley estatutaria 1581 de 2012, destinada al tratamiento de datos en bases de entidades de carácter tanto públicas como privadas, con un ámbito de

aplicación para el territorio nacional acorde a lo estipulado en el artículo 15 constitucional, en el entendido de que todas las personas tienen derecho a su intimidad personal y familiar, siendo el Estado el primer llamado a salvaguardarla, con en el compromiso de definir los límites entre lo público o privado, último elemento que corresponde al interés exclusivo de la intimidad de la persona física.

Esta ley estatutaria excluye los datos personales de carácter doméstico o personal, como también los regulados por la ley 79 de 1993 en la ley de censos, además de los datos impersonales de la ley 1266 de 2008, también los relativos a actividades meramente editoriales, periodísticos, los de inteligencia y contrainteligencia de la ley 1621 de 2013 y otros que conciernan a la defensa al lado de la seguridad del Estado. El dato personal es definido en la Ley 1581 como; Cualquier información vinculada que pueda asociarse a una o varias personas naturales determinadas o determinables. (Ley 1581 de 2012). Pudiendo ser de carácter no sensible o que no requieren consentimiento para su tratamiento y datos personales de carácter sensible que pertenecen a un grupo especial de datos regulados en el artículo 5 y siguientes como categoría especial bajo la definición de datos sensibles.

> Se 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 (Ídem, articulo 5).

El termino dato sensible así desarrollado, tiene un precedente Constitucional en la sentencia C-1011 de 2008, con conexión directa a derechos como la protección fundamental a la intimidad e integrando en esta condición de sensibilidad en la información "la relacionada, entre otros aspectos, con la orientación sexual, los hábitos del individuo y el credo religioso y político. En estos eventos, la naturaleza de esos datos pertenece al núcleo esencial del derecho a la intimidad," (Proyecto de Ley estatutaria de Habeas data, 2008). El artículo quinto de la ley estatutaria, también dispone la prohibición por acción u omisión de cualquier tipo de atentado o vulneración al derecho a la igualdad del artículo 13 Constitucional, comprendido en el sentido de realizar conductas discriminatorias que sitúen a las personas físicas o grupos de estas en condiciones de exclusión motivados en asuntos; raciales, étnicos, biológicos, o creencias sean estas de índole religioso, filosófico, político. Situación en la que de encontrarse cualquier persona supondrá para él un escenario desfavorable que le impida gozar de derechos o de ejercer sus íntimas convicciones, así como el libre desarrollo de su personalidad.

La sentencia C-748/11 integro a la definición de datos sensibles aquellos que llegasen a suscitar la "pertenencia a grupos u organizaciones sociales, de Derechos humanos o que promuevan intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición." (Sentencia C-748 de 2011). Subrayado que se integra motivado en atención a entender a este grupo poblacional a estar dispuesto a un ambiente notable de vulnerabilidad por ser víctimas de delitos que atentan contra su existencia física e integralidad emocional. El artículo estatutario contempla también los datos relativos a la salud en donde se incluyen por obvias razones la historia clínica de las personas, los relativos a la vida u orientación sexual. Finalmente se relacionan los datos biométricos entendidos estos como: "datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características

físicas, fisiológicas o conductuales de una persona que permitan o confirmen la identificación única de esta, como imágenes faciales o datos dactiloscópicos" (Reglamento del Parlamento Europeo y del Consejo, 2016)

8.3 Excepciones

Existen excepciones para el tratamiento de datos sensibles a tenor del artículo 6 de la ley 1581, observados en eventos donde el titular consienta en su tratamiento, como suele ser práctica común en la captación de datos con técnicas de identificación biométricas. Otra excepción se contempla en lo que es denominado dato público o cuando su captación se realiza en los escenarios en donde por disposición legal dichos datos son de tal carácter y solamente bastara informar la existencia del sistema, sin tener necesidad de solicitud de consentimiento para su tratamiento, por ejemplo el sistema de transporte masivo de Medellín, anuncia a los usuarios la disposición de cámaras y la captación de imágenes que serán almacenadas por un periodo de siete días. Una excepción más se hace en virtud de protección a la seguridad nacional, la democracia, los derechos humanos y las dispuestas en el desarrollo de actividades de inteligencia y contrainteligencia contempladas en los artículos 2 y siguientes de la ley 1621 de 2013.

También en el artículo 6 estatutario se adiciona la protección a intereses vitales que una persona requiere estando en incapacidad legal o física para auxiliarlos, prosigue este artículo con la excepción para actividades legítimas en el orden público o para procesamiento de asuntos de tipo judicial. Para el deber de informar que se materializa en el responsable del tratamiento Sentencia C-1011 (2008), existe una instrucción en el sentido de manifestar el carácter facultativo de la respuesta cuando se trate de datos sensibles de niños, niñas y adolescentes.

Finalmente la SIC (Superintendencia de Industria y Comercio) podrá imponer en uso de sus potestades sanciones cuando se traten indebidamente datos sensibles, que conllevaran definitivamente al cierre total de las operaciones, negocios o contratos en donde estos se involucren.

7.4 Comunidad Europea-España

Bajo este concepto (EU) se designa la unión de 28 países del continente europeo –hoy con la exclusión del Reino Unido- allí el rastreo del concepto dato sensible, es en tal sentido un tanto dispendioso, máxime si se tiene en cuenta que cada país de manera independiente manejaba hasta antes de la entrada en vigencia del RGPD, su propio argot legal para referirse a la protección de este tipo de datos, es por ello que quizás el primer intento de ubicar el concepto está consignado en el artículo octavo del Convenio para la protección de los derechos humanos y las libertades fundamentales, legislación que se expresó para el caso en el sentido de que "Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y su correspondencia" (Convenio para la protección de los derechos humanos y las libertades fundamentales, 1979). Argumentando tal disposición en la inestabilidad política de la Europa de posguerra que se tradujo en mecanismos para ayudar a la unión entre los pueblos, así mismo como paliativo al desarraigo de las familias, (Sentencia 28 de mayo de 1985, párr. 65.) de igual modo se aplica el ámbito de protección a la privacidad para las diásporas étnicas y a los individuos o grupos que pudieron haber quedado segregados, haciéndose extensiva para integrar el constante flujo de ideas, de creencias religiosas o activismos políticos que caracterizó este periodo.

El convenio también plantea causales de excepción para la no aplicación por parte de los Estados miembros, diseñando tópicos sobre los cuales y solamente cuando medie una necesidad de tipo legal de seguridad pública del Estado o en asuntos relativos a procesos judiciales, salud, prevención de transgresiones penales de los individuos, pueda ser válido vulnerar este derecho otorgado a las personas naturales. Otro aporte importante para la protección de la vida privada es el concerniente al tratamiento del tipo de datos que actúen de forma automatizada desarrollado en el Convenio 108 del Consejo de Europa del 28 de enero de 1981. Este instrumento realiza la definición de datos de carácter personal como; "cualquier información relativa a una persona física identificada o identificable" o "persona concernida" (Estrasburgo 28 de enero de 1981. p, 10.) Acercándose a una definición de datos sensibles en su artículo sexto, a modo de categoría particular de datos prohibiendo el tratamiento automático sin la necesaria garantía legal:

> "Los datos de carácter personal que revelen el origen racial, las opiniones políticas, las convicciones religiosas u otras convicciones, así como los datos de carácter personal relativos a la salud o a la vida sexual, no podrán tratarse automáticamente a menos que el derecho interno prevea garantías apropiadas. La misma norma regirá en el caso de datos de carácter personal referentes a condenas penales." (Artículo, 6, Ídem.)

Posteriormente la directiva 95/46/CE asume una definición de datos sensibles bajo la denominación de categoría especial de datos, lo hace con un mandato claro dirigido a los Estados miembros de prohibición del tratamiento sin justificación legal de los datos de carácter personal o de los que en todo caso revelen: El origen racial y étnico, las opiniones políticas, las convicciones religiosas, filosóficas, la pertenencia a sindicatos, así como el tratamiento de los

datos relativos a la salud o a la sexualidad. (Parlamento y del Consejo, de 24 de octubre de 1995). Detallando a continuación situaciones permitidas para el tratamiento o acceso en las que se incluyen grosso modo iguales situaciones a las planteadas en la ley 1581 ya abordada, con algunas modificaciones como las relacionadas al derecho laboral, además de establecer las facultades que los Estados miembros tienen para variar la aplicación de la directiva en razones de defensa o seguridad nacional. Es importante resaltar que en este instrumento, las consideraciones referentes a los desarrollos de la ciencia informática con técnicas de identificación biométricas, son tipos de datos que se entienden en lo sucesivo integrados en sus disposiciones, pero excluyendo, como es reiterativo en la normatividad abordada, los concernientes a la seguridad pública o defensa del Estado. La directiva aporta otro ingrediente importante para la protección de datos en el área periodística en donde se involucren imágenes, en el entendido de blindar la libertad de expresión y de información para que los Estados las armonicen con el derecho a la intimidad de las personas físicas.

En el ámbito penal existe otra herramienta legal que considera el procesamiento de datos sensibles en rigor y se refiere a la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, la cual tiene como objetivo el tratamiento de datos de carácter personal con fines de prevención, investigación, detección, enjuiciamiento, ejecución de infracciones penales o amenazas contra la seguridad pública. Los datos denominados sensibles están contemplados allí en el décimo artículo como categorías especiales de datos personales, de igual modo traen como novedad el considerar los datos genéticos y biométricos, también se relacionan las excepciones legales de acceso o tratamiento en los eventos puntuales establecidos vale decir; por autorización expresa, en protección de intereses vitales o cuando el titular los hiciere a su voluntad públicos. (Directiva (UE) 2016/680)

Finalmente, el último escaño de la legislación europea para la protección de datos es aportado por la Directiva (UE) 2016/679 del Parlamento europeo y del Consejo, del 27 de abril de 2016, legislación más conocida con el nombre genérico de Reglamento General de Protección de Datos. (Reglamento (UE) 2016/679) En adelante RGPD, el cual es una apuesta de vanguardia sancionada como Ley el 27 de abril de 2016, con entrada en vigencia a 25 de mayo de 2018. Esta legislación pretende el cuidado de los temas relacionados con los datos personales, de su protección ante el auge inusitado de las tecnologías informáticas y la masiva generación de datos a través de las redes, dispositivos, entre otras muchas fuentes. El RGPD propone una concentración de la normatividad en el ámbito del continente europeo en un solo instrumento, no con el alcance de Directiva porque el objetivo de protección ya está logrado, si no en el entendido de ser considerado reglamento como instrumento de Ley vinculante para el territorio de la (EU).

Como dato personal se considera inicialmente en el RDPD; "toda información sobre una persona física identificada o identificable que conduzca a identificarlo, elementos que pueden ser el nombre, el lugar de residencia, el número de identificación", (Numeral 1, Articulo 4, ídem). Datos que corresponden en un primer momento a la función social y económica que estos deben cumplir, tal como se indica en sus consideraciones en donde de igual forma se resalta, la necesidad de respeto hacia la privacidad de las personas, de su vida familiar, de las garantías fundamentales, las libertades y principios establecidos en los tratados. Contexto que debe ser la base para una clase preferencial de datos denominados personales especiales.

Así los datos sensibles considerados con anterioridad en los diferentes ordenamientos, en el RGDP son un término de referencia dispuesto literalmente a tenor de esta categoría "El presente Reglamento reconoce también un margen de maniobra para que los Estados miembros

especifiquen sus normas, inclusive para el tratamiento de categorías especiales de datos personales («datos sensibles»).” (Ibídem, Núm. 51).

Las categorías especiales de datos personales son entonces sinónimo de datos sensibles sobre los cuales se instruye para su tratamiento en el artículo noveno disponiendo el siguiente contenido:

> “Quedan prohibidos el tratamiento de datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientaciones sexuales de una persona física.” (Artículo 9, Ídem).

Difiere tal disposición a lo consignado en la ley 1581 en constituir esta ultima en los datos sensibles aquellos que afectan la intimidad del titular o cuyo uso indebido genere su discriminación, de igual modo el aporte realizado por la sentencia C-748/11 al integrar los datos relativos a la pertenencia a organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o garanticen los derechos y garantías de partidos políticos de oposición (Ídem, articulo 5).

8.6 Excepciones

Están excluidas de la anterior apreciación todas aquellas disposiciones de los Estados miembros para el ejercicio de sus funciones y de manera especial en atención al interés público. También cuando el titular de su consentimiento expreso, en el ámbito de la salud para garantizar la eficacia de un servicio, de igual modo para la salud pública cuando esta lo amerita. “Este

tratamiento de datos relativos a la salud por razones de interés público no debe dar lugar a que terceros, como empresarios, compañías de seguros o entidades bancarias, traten los datos personales con otros fines. (Numeral 55, consideraciones, ídem). Así mismo en el régimen de seguros o para la investigación científica, histórica, estadística, finalmente para la defensa y reclamaciones en procesos judiciales.

En síntesis; el RGPD tiene la potestad de unificar el tratamiento, la libre circulación, la recolección de datos, con la finalidad de proteger a las personas físicas como también sus datos personales, esto al margen de la nacionalidad o sitio de residencia pero especialmente frente al Estado, las empresas que con el direccionan o los medios de comunicación, brindando para este propósito seguridad jurídica y transparencia.

Para Edward Snowden el listón del GRPD se ha colocado demasiado bajo, opina este activista de la protección de datos, que el problema no es la captación si no su almacenamiento. El RGPD o todas las regulaciones pertinentes en cualquier contexto deben tener como soporte que la obtención del dato fue realizada bajo los parámetros correctos que suponen la protección a garantías fundamentales por tal motivo su almacenamiento no comprometería a futuro una imposición de peligro para el titular, quien como solución debe conservar la acción para que los Estados o los particulares que los almacenan blinden sus datos evitando que estos se filtren y estén disponibles para su control (Ranger, 2019).

8.7 Estados Unidos

La protección de datos en este país tiene como rasgo distintivo en comparación con el ámbito europeo, la laxitud de las normas, no en vano es el país de las libertades de igual modo uno de

los ordenamientos en donde más pueden recabar las políticas y estrategias para la seguridad nacional. En los E.U tienen asiento las mayores empresas que capturan, procesan o almacenan datos, así mismo el comercio realiza transacciones voluminosas por estos medios, intereses que evidencian la dificultad para concretar como en el caso de la comunidad europea una legislación que unifique la protección de datos. No obstante, se tiene el precedente en leyes tanto estatales como federales para determinados sectores sociales y económicos que se preocupan por el tema. (Amazon. Citado por Vivian Newman Pont, María Paula Ángel Arango. (2019). (p. 10)

- **La Ley Hipaa:** El Congreso E.U. Health Insurance Portability and Acounttability Act, agosto 21 de 1996. Es un primer ejemplo, básicamente esta ley regula la protección o seguridad para el acceso a la información, además de la privacidad o derecho que tienen las personas para que este tipo información no se haga pública en asuntos relacionados con su salud. En esta legislación se dispone quien o cuales personas, a razón de que negocios o transacciones pueden tener acceso a los datos. Son reglas de confidencialidad que se hacen extensivas inclusive a las conversaciones con él personal médico, ampliando el denominado secreto profesional. El objetivo de Hipaa es limitar el uso de este tipo de información también penalizar a quienes infrinjan sus disposiciones. Hipaa es una ley de carácter estatal aprobada por el Congreso en 1996, es vinculante en los 52 estados incluido Puerto Rico, la clase de datos que protege están clasificados en las series; escritos, papeles, con voz, sin importar la calidad, tamaño o formato, tiene ámbito de aplicación para protección de datos dentro y fuera del punto de atención en cualquier calidad de sujeto responsable, la Hipaa también armoniza con el título VI del Civil Rights Act. En el sentido de no estar exentos los responsables en denegar cualquier

actividad con base en motivos de; “race, color or National origin”. (Ley de derechos civiles, 1964).

8.8 Excepciones

En asuntos de prioridad pública, o cuando se exige por ley, para cuestiones en derechos laborales, en actividades de supervisión de la salud privada o pública, para actividades de investigación con funciones especiales del gobierno, para defunciones y la donación de órganos. (Departamento de Comercio de los Estados Unidos).

- **Privacy Shield Policy:** La protección de datos bajo este instrumento se realiza de una forma que puede denominarse sectorizada, por que atiende en primera instancia a la legislación propia que constituye el marco legal del escudo de privacidad, otro aspecto de esta política es la regulación y autorregulación de las empresas que se adhieren o la adoptan para certificar las transferencias de datos.

  El escudo de privacidad es un mecanismo que permite a las organizaciones de derecho privado, hacer negocios en U.S con empresas europeas, así como el tratamiento de datos personales de individuos de la UE y Suiza, para estos eventos el departamento de comercio de U.S ha elaborado una lista de autoridades certificadas en la protección de datos de las personas físicas, en cuya calidad en el suplemento de los principios establece la consideración de datos sensibles en los términos diseñados por la Directiva 95/46/CE. A todo esto, es de tener en cuenta que el privacy shield policy se ejecuta desde enero de 2017 cuando aún no entraba en rigor el RGPD es por ello que hoy en los U.S se están

rediseñando leyes que armonicen con las disposiciones del reglamento en el entendido de integrar los nuevos conceptos emanados.

- **California Consumer Privacy Act**: Es la denominación de la más reciente propuesta legislativa para la protección de datos, el CCPA por sus siglas en inglés, es un proyecto de ley que se agrega al título 1.81.5 del Código Civil, fue aprobado el 18 de junio de 2018 con vigencia a partir del primero de enero de 2020. El California Consumer Privacy Act. Ley de privacidad del consumidor de California de 2018, es en síntesis una Ley que protege la privacidad en definidos contextos, pero de manera muy especial atina a las transacciones de datos que se realicen con apoyo en plataformas de comunicación virtual o a través de internet en el entendido de que en estas, las empresas que direccionan; "Es posible que sepan dónde vive un consumidor y cuántos hijos tiene, qué tan rápido conduce un consumidor, su personalidad, hábitos de sueño, información biométrica y de salud, información financiera, información precisa de geolocalización y redes sociales, por nombrar algunas categorías." Las empresas están obligadas a diseñar sus propias políticas de privacidad, darlas a conocer al consumidor o cliente. Explicitando el propósito, categorías de datos, las fuentes de las cuales se puede recopilar. En que eventos se pueden compartir, el derecho que tiene el cliente de conocer qué tipo de datos o información personal se almacenan sobre él, si se venden o se divulgan y a quien.

"Información personal" significa en el CCPA la que identifica, se relaciona, describe, es razonablemente capaz de asociarse o podría vincularse razonablemente, directa o indirectamente, con un consumidor u hogar en particular." Para contrarrestar arbitrariedades los consumidores tendrán en sus manos un instrumento que les da potestad de exigir a las empresas, el ejercicio de

actividades y procedimientos dirigidos a la protección de sus datos. Se incluye también una cláusula de igualdad en el servicio y precio. Para evitar posibles retaliaciones por el uso del recurso. En el CCPA, no existe una definición explícita de datos sensibles, se infiere si del contenido de la ley que estos se atribuyen a la misma calidad de datos estipulada en el RGPD, habida cuenta de la pretendida integración y armonización de las dos disposiciones.

8.9 Excepciones

En la información personal no se incluye la que es de tipo pública o legalmente disponible en los registros gubernamentales," Disponible públicamente" no significa información biométrica recopilada por una empresa sobre un consumidor sin su conocimiento. (Numeral 2, literal o, ídem. El énfasis es nuestro).

CAPITULO II

8. Los derechos a la privacidad, a la intimidad y a la propia imagen

9.1 Derecho a la Privacidad

- **Antecedentes del Derecho a la Privacidad**

El derecho a la privacidad tiene su impronta en el common law, explícitamente en Inglaterra donde es presentado a partir del caso Semayne con el célebre aforismo; “a man’s house as his castle” (Indiana 2003), mediante el cual Edward Coke (1604) aprueba la defensa que hace Richard Gresham de su domicilio ante la ilegal arremetida del sheriff para ingresar y obtener documentación. El juez Coke, reivindica en su consideración la invulnerabilidad del hogar frente a cualquier invasión arbitraria de la privacidad, especialmente cuando esa intromisión

proviene del Estado, se asegura así la protección de bienes como la propiedad privada, la documentación, la intimidad familiar, en el entendido de que no es plausible vulnerar la esfera íntima de las personas con el propósito de obtener evidencias para un caso, cuando no medie una causa legítima o un consentimiento expreso de la voluntad del titular.

Este razonamiento jurisprudencial transpuso el atlántico para recabar en el derecho procesal de las colonias, como ejemplo es retomado por el segundo presidente de los U.S; John Adams, en el caso James Otis al expresar "A man's House is his castle; and whilst he is quiet, he is as well guarded as a prince in his castle". (Adams, 1865)

También se depositó en la Constitución de los de los U.S a partir de las diferentes enmiendas donde jurisprudencialmente se ha interpretado e integrado, así; en la primera enmienda puede verse protegida la privacidad en las creencias religiosas, políticas o filosóficas de las personas, en la tercera se avoca por la protección a la vida familiar y del hogar, la cuarta hace relación a requisas o requerimientos arbitrarios por parte del Estado, la quinta enmienda se manifiesta frente a la no autoincriminación o abstenerse de revelar información privada, en la novena se hace énfasis en la negativa por parte del Estado a interpretar otros derechos. (Griswold v. Connecticut, 1965). Finalmente, la decimocuarta se pronuncia en relación con el debido proceso para que ningún Estado o autoridad pueda sin la observancia de este principio privar de la vida, libertad o propiedad a ninguna persona.

Igual posición hermenéutica es utilizada un centenar de años más tarde por el juez Cooley al establecer un ensamble entre las diferentes interpretaciones de las enmiendas constitucionales

en el entendido de que todas finalmente confluyen en la protección de la libertad de la persona, de su vida con dignidad, así como de su propiedad, todo esto allende a la disposición de que sin causa o por medio de una orden judicial ilegitima puedan hacer el Estado y los medios de

comunicación. Conceptos que finalmente se sintetizan en el derecho autónomo a ser dejado solo o "let to be alone" (Cooley, TH. M 1868). O sea, la garantía de ser dejado a solas, no por la religión, la moral o la filosofía, sino por el Estado, para asegurar la determinación autónoma de su conciencia cuando toma las decisiones requeridas para la formulación de su plan de vida en todas las dimensiones fundamentales de ella" (Citado por Patricio Marianello. En Criterio Jurídico Santiago de Cali V. 13, No. 2 2013-2 pp. 132).

Este inventario conceptual y legislativo es base del hito fundacional del derecho a la privacidad por vía doctrina, que es abiertamente planteado a partir del escrito; "The right to Privacy" (Brandies, 1890) de los abogados estadounidenses Samuel Warren y Louis Brandies. En este escrito los juristas se manifestaban inconformes ante la intromisión indebida en su vida y asuntos particulares al ver menguada la calidad de la misma por ser vulnerada en su dignidad especialmente por los medios de comunicación y las nuevas tecnologías llámese para el momento: fotografía, prensa, telégrafo.

Ante esta invasión no consentida, el escrito propone diques de contención como los relacionados a lo que un individuo de manera autónoma expone al público, se trata en definitiva de resaltar la protección a las personas, su libertad, propiedad, públicamente resumidos en el derecho a disfrutar la vida, rechazando expresamente cualquier conexión con la libertad o propiedad y ubicando este derecho en la categoría de derecho individual autónomo.

Este hito fundacional y doctrinario de la privacidad, permitió un desarrollo posterior en la jurisprudencia con casos en los que se consideran diferentes facetas o niveles, ver (Olmstead v.The United States, 1928) en donde se decide acerca de la cuarta enmienda y su no violación en un caso de escuchas telefónicas por considerar que las conversaciones fueron voluntarias y entre las partes. Argumentos posteriormente refutados en (Katz v. The United States, 1967), indicando que la cuarta enmienda protege las personas no los lugares –cabina telefónica- e introduciendo

el concepto de expectativa razonable para su cumplimiento. La proximidad física como requisito es analizada en el caso (Osborn V. United States, 1966). Entonces en los U.S el derecho a la privacidad se ha configurado desde la doctrina y a través de la jurisprudencia, no existiendo propiamente en la Constitución una designación expresa para él, pues se ha construido mediante la interpretación de enmiendas fundamentalmente la primera, la cuarta, y la decimocuarta. Última de especial apreciación por hacer referencia a la libertad de elección individual y como núcleo intangible de su protección derivada del debido proceso legal sustantivo.

Sin embargo, donde realmente puede verse plasmado de forma notoria el derecho a la privacidad en los U.S, es en la protección de la denominada información personal, regulada en disposiciones contenidas en la Ley de privacidad de 1974 y las que le modifican complementan o adhieren. En tal contexto también se puede afirmar que la protección a este derecho está reglamentada de manera parcial en leyes y algunas constituciones estatales como California, Illinois, Nevada, o Hawái, en donde la Corte ha estimado la protección de la información y de su confidencialidad, en el entender que existen asuntos privados del individuo que este no quiere y no pretende hacer público;

> "Las relaciones sexuales, por ejemplo, son asuntos completamente privados, como lo son las disputas familiares, enfermedades desagradables, vergonzosas o humillantes, las cartas personales más íntimas, la mayoría de los detalles de la vida de una persona, o en su hogar, y algunos de su pasado que preferiría olvidar" (Constitución de Hawái, Carta de derechos, preámbulo, numeral 5)

También está dispuesto este derecho en normas federales que incluyen invariables y múltiples excepciones, con el agravante de las lagunas o vacíos que sería engorroso, dispendioso

o en ocasiones inútil el tratar de citar o compendiar. Vale resaltar el esfuerzo por integrar este derecho para ser tratado de forma constitucional, voluntad que puede vislumbrarse a partir de propuestas jurisprudenciales o sentencias como es el caso de (Whalen v. Roe 1977) que se refiere a posibles demandas de personas en contra del estatuto de 1972 de Nueva York para el control de las drogas potencialmente peligrosas, y en la que los apelantes arguyen una eventual violación al derecho a la privacidad constitucionalmente protegido al permitir registrar su nombre o datos en una base usada para el control de distribución de los medicamentos. Los apelantes se oponen para este propósito en intereses como son:

El interés individual en evitar la divulgación de asuntos personales, el interés en la independencia para tomar ciertas clases de decisiones importantes y libres de la compulsión gubernamental. Y el derecho del individuo a ser libre en sus asuntos privados de la vigilancia e intrusión gubernamental, y protegido por la cuarta enmienda. (Whalen v. Roe ídem nota 24)

9.2 Definición del Derecho a la privacidad

La real academia de la lengua define la privacidad como; cualidad de privado ó ámbito de la vida privada que se tiene derecho a proteger de cualquier intromisión.

En el common law se define así: “El derecho a ser dejado solo, a vivir la vida que uno elige, libre de agresión intrusión o invasión, a excepción de las que puedan estar justificadas por las necesidades claras de la vida en comunidad bajo un gobierno de leyes”. (Inc. v. Hill, 1967) La Corte Suprema de los U.S reconoció de la misma manera el talante constitucional de esta garantía en el caso (Griswold v.Connecticut 1965) “como el derecho que asiste a toda persona a tomar las decisiones que afecten a su vida privada”. La vida privada se concibe entonces como un campo en donde el individuo decide complementar y girar alrededor de un pequeño

dispositivo social llámese familia o comunidad. Para crear dentro de este unas relaciones que incluyen la cordialidad, la ayuda, la confianza, lo privado evade así el espacio de lo público excluyéndole del conocimiento del tipo de relaciones y circunstancias que acaecen al interior del estrecho círculo de relaciones sean estas familiares, profesionales, de pertenencia a determinados grupos o las que atañen directamente al individuo.

La Corte Constitucional de Colombia, por su parte define a la privacidad o el ámbito de lo privado en la sentencia T-787 (2004) como "los asuntos que en principio tocan exclusivamente con los intereses propios y específicos de la persona humana sin que afecten o se refieran a los demás miembros de la colectividad" (Corte Constitucional. 18 de agosto de 2004, M.P: Rodrigo Escobar Gil, Sentencia T-787 de 2004), consideración que armoniza con la anterior en el entendido de establecer el antagonismo propio de la relación público -privado.

Para el contexto europeo la privacidad y la intimidad están indisolublemente ligadas, e inclusive se postula la teoría de sinonimia a partir del texto de W&B, según se desprende de la traducción realizada al castellano. No obstante, la definición más próxima del concepto privacidad y vida privada esta compendiada en la doctrina del TDHE en la cual se considera que sintetiza la protección psíquica, moral y física de la persona. Un evento palpable es lo considerado en el caso Niemietz v Alemania donde la Corte se pronuncia en el sentido de no dar una noción integra de vida privada por considerar que:

> "Sería demasiado restrictivo limitarla a un "círculo íntimo "donde cada uno pueda conducir su vida personal a su gusto y excluir enteramente el mundo exterior de este círculo. El respeto de la vida privada debe también englobar, en cierta medida, el derecho del individuo de anudar y desarrollar relaciones con sus semejantes" (Sentencia de 16 de diciembre de 1992, Niemietz c. Alemania, n° 13710/88)

Esta consideración se basa en lo dispuesto en el artículo 8 de CDEH en el entendido de querer armonizar la protección de la unidad familiar, documentos, domicilio, y en la certeza de no haber cesación en la custodia de estas garantías ni por injerencia estatal o de los medios de comunicación. A no ser los requisitos legales establecidos, en los que se incluyen la seguridad nacional y las que atañen a las demás libertades. En resumen, el concepto de privacidad es un espacio distinto a la definición de intimidad, en las diferentes legislaciones pueden ser sinónimos en su consideración como en el caso colombiano en donde está consignada en el artículo 15 de la CN, igual apreciación basta para el ámbito europeo en donde como se ha visto está regulada en el artículo 8 del CDEH, En estados unidos en contraste se presenta el fenómeno inverso al considerar el termino privacidad, más no intimidad. En síntesis, el derecho a la privacidad demarca el derecho a la vida privada particular y familiar que el Estado y las personas deben respetar y entre las cuales se incluye la intimidad personal.

9.3 Derecho a la Intimidad

- **Antecedentes del derecho a la intimidad**

Los antecedentes del derecho a la intimidad son ambiguos ya que en muchos casos como se ha señalado antes; intimidad y privacidad son sinónimos, así el concepto de privacidad reseñado previamente y desarrollado a partir de la doctrina de W&B por la jurisprudencia de los E.U, es la columna o baluarte a partir de la cual se ha estructurado la evolución del derecho a la intimidad, descansan en ella todas las apreciaciones o variaciones tanto semánticas (Benigno Pendas, 1996, p.17) como de los conceptos jurídicos de los nuevos espacios o ámbitos de aplicación que se le han integrado, esto básicamente porque en el common law la privacidad tiene como sustrato a la Libertad, que en sus inicios protegió originalmente el anonimato, la

soledad, la autonomía personal, la propiedad, pero expandiéndose después a aspectos como la libre expresión, la reputación, la imagen, el honor. Mientras la Intimidad tal como se ha desarrollado en los ordenamientos jurídicos continentales se asume como un derecho Constitucional fundamental con cimiento en la dignidad humana, por tanto manifiesta su interés y resalta los asuntos relativos al cuerpo de la persona, al desarrollo de la personalidad con los eventos que a este conciernen como son las sensaciones, emociones o sentimientos del ser humano.

- **Definición del Derecho a la intimidad**

En la jurisprudencia colombiana existen múltiples definiciones si se tiene en cuenta los contextos en los que se quiera abordar, el artículo 15 constitucional la expone en sentido de que: "Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre". (Constitucion Política de Colombia, 1991). Disposición no muy clara puesto que la coteja con otras garantías como el buen nombre, haciendo un llamado al Estado para que las proteja tanto en la persona como en la órbita familiar, se complementa el artículo con el habeas data. Todos ellos son considerados derechos autónomos.

La Corte Constitucional, para nuestro ámbito de injerencia y estudio, que no es otro que la vulneración de este derecho por parte del Estado en asuntos concernientes a su seguridad, en la sentencia C-540 2012 del proyecto de ley estatutaria para el fortalecimiento del marco jurídico para el desarrollo de actividades de inteligencia y contrainteligencia, ha definido el derecho a la intimidad como:"El espacio intangible, inmune a las intromisiones externas, del que se deduce un derecho a no ser forzado a escuchar o a ver lo que no desea escuchar o ver, así como un derecho a no ser escuchado o visto cuando no se desea ser escuchado o visto." (Ibídem).

El derecho a la intimidad tiene como característica principal el ser un derecho disponible, en el entendido de que corresponde a cada titular decidir a voluntad que parte de su contenido quiere hacer público, la esencia del derecho a la intimidad engloba niveles que alcanzan lo personal, familiar, social, profesional o gremial. Los límites al derecho a la intimidad están identificados como intrusiones ilegitimas en la vida privada o en la esfera personal, así como las difamaciones e información falsa y la divulgación de información privada en reserva. La doctrina también ha definido el derecho a la intimidad como el espacio de la personalidad de los sujetos que no puede ser, salvo a propia elección, de dominio público. (Novoa Monreal, 1971)

En Europa, la intimidad está considerada derecho fundamental en el artículo 18.1 de la Constitución española, allí es estimada conjuntamente con la inviolabilidad del domicilio, recubriéndose con la propia imagen, el honor personal y familiar, son considerados además derechos autónomos. El objetivo principal de este artículo es el respeto por la intimidad personal frente a cualquier injerencia del Estado o particulares, también de cara a una publicidad no requerida, busca igualmente salvaguardar la dignidad, así la protección al derecho a la intimidad; "Garantiza un derecho al secreto, a ser desconocido, a que los demás no sepan que somos o que hacemos, vedando a terceros a que decidan los límites de lo privado, reservando a cada persona un espacio ajeno a la curiosidad, cualquiera sea el contenido de esa esfera" (Sentencia 127/2003 de 30 de junio)

El considerar el derecho a la intimidad como un derecho fundamental garantiza a la persona la tutela de protección por parte del Estado, de igual modo le da una carta que posibilita el ejercicio de la acción subjetiva para reclamar, colocándole en una posición de ventaja frente a cualquier lesión por parte del estamento público o a cargo de particulares estableciendo límites y condiciones de acceso a la información que él considera intima porque: "A nadie se le puede

exigir que soporte pasivamente la revelación de datos, reales o supuestos, de su vida privada personal o familiar" (Sentencia 134/1999 de 15 de julio). Finalmente el convenio para la protección de derechos humanos y las libertades fundamentales (CEDH) en el artículo 8 hace alusión al derecho que tiene toda persona por el respeto de la vida privada y familiar, para tal fin la jurisprudencia ha desarrollado diversas esferas de tratamiento de las cuales las más íntimas corresponden a los pensamientos, sentimientos , emociones que un individuo ha expresado de manera confidencial, materias que según el tribunal Constitucional de Alemania constituyen una protección intangible en pro de la dignidad humana.(Sentencia BVerfG, 31.01.1973)

8.4 Derecho a la propia Imagen

- **Antecedentes del Concepto de derecho a la propia imagen**

En el Derecho el concepto de imagen es "toda expresión que haga sensible un objeto carente en sí mismo de susceptibilidad para manifestarse, el derecho a la propia imagen es un derecho innato a la persona y uno de los atributos de la personalidad" (Gritama, 1962). El derecho a la imagen tiene un desarrollo autónomo e independiente, múltiples son las facetas y niveles que pueden ser considerados para analizarlo, su desarrollo como garantía constitucional se enlaza continuamente con relación al honor, la honra, la protección de derechos de autor, con el derecho a la información, también con los derechos que nos atañen como son la privacidad e intimidad. El derecho a la propia imagen no aparece como tal de manera explícita en la constitución americana, de igual modo que en la colombiana y su integración al ordenamiento se debe a interpretaciones jurisprudenciales o vía doctrina. Es considerado si de manera autónoma en las de Portugal, España, Brasil. (Rodríguez 2009 p. 29/48). En tal sentido en Colombia no se define explícitamente el derecho a la imagen como fundamental y venido el caso se analiza, sea de manera individual o

integrándolo de modo concurrente con otros derechos, siendo no obstante de desarrollo jurídico reciente, situación que se plasma como ejemplo en la sentencia T-408 1998 que considera el derecho a la propia imagen como atributo de la personalidad relacionándolo directamente con lo dispuesto en el artículo 14 constitucional.

En otro contexto cuando se trata de su proyección dinámica, el derecho a la imagen se enmarca en el libre desarrollo de la personalidad del artículo 16, y con relación al artículo 15 es concurrente el derecho a la propia imagen con el derecho a la intimidad cuando se divulga sin consentimiento contenidos o datos propios de esta. (Tutela T-233 de 2007, Colombia). El derecho a la propia imagen en Colombia está definido en síntesis como "un derecho autónomo que puede ser lesionado junto con los derechos a la intimidad, a la honra, al buen nombre de su titular, en cuyo ejercicio está estrechamente vinculado a la dignidad y libertad de la persona"(Tutela T-634 de 2013, Colombia). En Colombia la protección del derecho a la imagen es de tipo casuístico su vulneración se debe a la falta del consentimiento para su tratamiento, del mismo modo que del desconocimiento por parte del titular de la finalidad. Existe un índice sentimental o moral, no a todas las personas se les interpreta con igual rasero, ni pueden aspirar a compensación económica debiendo comprobar los daños morales para tal efecto.

En los U.S no existe el derecho expreso a la propia imagen; se habla en este ordenamiento del right of privacy ya abordado, o más comúnmente para esta materia del right of publicy, en ese país este derecho tiene un tinte económico "El valor de la imagen de por sí es inminentemente patrimonial" (Barnett, 1999, p.559). Atendiendo de esta forma a la calidad de la persona para medir su grado o nivel de afectación, por lo cual la consideración de esta garantía para su compensación se ha vinculado también como contraparte del derecho a la información y la libre expresión, aunque recientemente para el reclamo subjetivo mediante una causa de acción

privada se omite la consideración a la importancia de la persona en virtud de la nueva ley anti paparazzi (Statutory Civil Law) que autoriza a cualquier individuo sin reparo a su valor , pero que ha sufrido un intrusión física o constructiva en su privacidad con el fin de obtener o captar su imagen a interponer este tipo de recurso. Los Estados en el país americano, brindan una protección al derecho a la imagen; en New York, puede verse nominada una defensa estatutaria, con fundamento en la Ley de derechos civiles artículos 50 y 51 (Mckinney 1976), donde está protegido bajo el presupuesto de que cualquier imagen reconocible, no solo una fotografía real, pueden calificar como un retrato o foto. Para acceder a la acción, el demandante debe probar que se usó su imagen, se hizo con finalidad comercial, además sin autorización por escrito del titular. En Nueva York como en muchos estados no se ha reconocido esta garantía como parte del derecho consuetudinario.

En California la ley estatutaria protege a la persona en su nombre, voz, firma, fotografía, semejanza. Código Civil, División 4, parte 1, titulo 2, capitulo 2, artículo 3, numeral 3334, literal b.

Allí la privacidad está considerada como derecho fundamental en el artículo primero: "Todas las personas son, por su naturaleza, libres e independientes y tienen derechos inalienables. Entre estos está perseguir y obtener seguridad, felicidad y privacidad.

Su desarrollo jurisprudencial en el derecho consuetudinario también se traza a partir del artículo de W&B, el derecho a la imagen es subsidiario al de privacidad y se presenta como uno de sus niveles en donde una persona víctima de la exposición ilegal de su imagen puede reclamar una causa de acción fundada en el derecho a la privacidad constitucional de California.

En la U.E, la constitución española considera expresamente este derecho en el artículo 18.1 desarrollado legislativamente en la Ley orgánica 1/1982 "Derecho al honor a la intimidad y a la propia imagen". Cada derecho como en los ordenamientos anteriores puede verse lesionado

de manera individual como concurrente. En España se considera a esta garantía fundamental en una relación muy próxima con el derecho de libertad de información y de expresión, lo cual se hace más evidente cuando se trata de personas públicas o reconocidas, en virtud a su "Imagen social". Sin embargo, a tenor del artículo octavo de LO 1/182, Numeral 2 lit. a, la captación de una imagen procederá sin consentimiento cuando: "se trate de personas que ejerzan un cargo público o una profesión de notoriedad o proyección pública de igual modo cuando la imagen se capte durante un acto público o en lugares abiertos al público." (España Ley 1/1982, de 5 de mayo, sobre protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen)Los casos en que la jurisprudencia se ha manifestado con precedente favorable implican la pretensión de tutela para su amparo por intromisión ilegítima en su derecho a la propia imagen, en: Las fotos más esperadas de Marta Chavarri y Alberto cortina, publicadas sin su consentimiento por la revista diez minutos.

En la Sentencia núm. 139/2001 de 18 de junio No se consideran intromisiones ilegitimas a tenor del numeral 1 del artículo 8, LO 1/182, las realizadas o acordadas por la autoridad competente de acuerdo a la ley, o en virtud de un interés histórico, científico o cultural relevante. El artículo 51 de RGPD resalta la consideración sobre las fotografías, a las que no considera una categoría especial de dato personal en relación con su tratamiento, a menos que se utilicen técnicas que permitan la identificación univoca de una persona, ejemplo pasaporte tratado con técnica de reconocimiento facial 2d, y en cuyo caso dicho tratamiento solo podrá ejecutarse con el exclusivo consentimiento del titular o en virtud de disposiciones legales o funciones públicas.

- **Definición del concepto del Derecho a la propia imagen**

"Es el derecho a controlar la captación, difusión y en su caso, explotación de los rasgos físicos que hacen reconocible a una persona como sujeto individualizado" RAE. En la doctrina el

derecho a la propia imagen se ha definido como: “El derecho a que nadie capte, difunda o utilice la imagen de una persona sin que esta lo autorice”. (Díaz, 1990). La imagen es junto con los atributos que la definen el rasgo más importante de la personalidad. (Villafañe Gallegos 2002) En la actualidad merced al tratamiento informático en dispositivos de captura es posible su obtención en volúmenes inconmensurables y de manera consecuente lograr su almacenamiento en forma de datos que pueden ser administrados por los Estados o empresas a su servicio.

El Derecho acerca la imagen al documento, así el artículo 243 del Código General del Proceso colombiano clasifica las diferentes clase o tipos de documentos en; mensajes de datos, fotografías, cintas cinematográficas, videograbaciones, y en general, todo objeto que tenga carácter representativo o declarativo, pudiendo ser públicos o privados. La imagen es considerada un documento de tipo descriptivo. (Sentencia 2017-00024 de 2018, Colombia).

Existe un consentimiento para el tratamiento de la imagen el cual es considerado en el artículo 9 del GDRP como dato personal sensible, el comercio puede hacerlo para ofertar sus productos y como práctica regulatoria en su seguridad con la advertencia visible del funcionamiento, la Policía y el Estado pueden sin consentimiento en sitios públicos. La información allí almacenada puede ser saqueada o hackeada mediante una reconstrucción del algoritmo que la genera y este puede ser mal utilizado, de ahí que pueda desprenderse un nuevo concepto Iusinfoormático de imagen, que es la de que tu imagen y tu personalidad han sido sustraídas u hurtadas. Los particulares pueden cometer delitos con el uso indebido de la imagen, el Estado vulnera Derechos Fundamentales. Nikken (1994).

Finalmente, en el contexto de este trabajo para la Ciencia informática y la Biometría la imagen es una representación en una matriz de dimensiones n x n = N, donde la imagen capturada es almacenada en forma de logaritmo. (Benavides et al. 2008).

CAPITULO III

9. Los datos biométricos

10.1 Concepto de biometría

"La biometría es una tecnología de seguridad basada en el reconocimiento de una característica física e intransferible de las personas, como la huella digital, que, al ser una característica única de cada individuo, permite distinguir a un ser humano de otro". (Concepto , 2013).

Como Biometría se conoce a la técnica mediante la cual se permite identificar las características principales de un individuo, en un cumulo de tipologías que integran no solo los aspectos físicos si no que posibilitan también almacenar rasgos del comportamiento y la conducta, datos que en conjunto pueden predecir los gustos, las necesidades, las acciones, los consumos, las expectativas de un individuo o de un grupo de personas, permitiendo al mismo tiempo realizar o trazar un perfil de estos.

> "La identificación biométrica es una tecnología de seguridad que mide e identifica alguna característica morfológica que nos diferencia del resto de seres humanos. Se usa para medir y analizar rasgos físicos o de conducta de un individuo y para verificar identidades. Se considera en la actualidad como el método ideal de identificación humana." (Biometria, 2013)

La biometría es una identificación automática en relación con particularidades biológicas y de conducta. En la actualidad la técnica de la biometría es variada con múltiples aplicaciones, pudiendo ser definida como una práctica en la cual convergen las tecnologías que se utilizan para la identificación o autenticación de las personas, estas tipologías pueden ser anatómicas y

estáticas como la mano, la huella, el iris, facial, características de comportamiento o dinámicas como la huella y la voz.

El dato biométrico se encauza en la corriente de dato personal sensible, así en el RGPD, es dato biométrico los: "datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos" (Numeral 14, Artículo 4, ídem.). Los avances del campo digital y de la informática han posibilitado la transformación de esta técnica en tecnología al utilizar otras áreas del conocimiento que confluyen para favorecer plataformas con habilidades para la captación de datos así mismo la predicción de posibles comportamientos o conductas. Entonces la sola captación de un rostro mediante un dispositivo de reconocimiento facial podrá desprender una serie de datos sensibles relacionados indicando de manera simultánea entre otras cosas el origen étnico, sexo, edad, ocupación, pertenencia a grupos o acercamiento a ideas políticas o religiosas, estado civil, orientación sexual, que enfermedades padece, si tiene antecedentes o ha sido condenado. Es decir, el cumulo integro de lo que se considera dato sensible.

10.2 Usos modernos de la biometría

La primera acepción moderna de biometría proviene de la Ciencia Estadística emergiendo como una técnica auxiliar de la bioestadística a modo de un procedimiento de contraste conductual y biológico que ayudaba a determinar el estudio de ciertas tipologías. Hoy el concepto está determinado como "El reconocimiento automático de los individuos en función de sus características biológicas y de comportamiento" (Valencia, 2018). Desarrollos posteriores de las técnicas biométricas, en el área y campo de la dactilografía finalizando el siglo XIX, ubican a

Juan Vucetich (Vucetich, 1904) quien en sendos trabajos dio instrucciones para la adopción de un sistema antropométrico basado en las impresiones dactilares de los individuos. Posteriormente, durante la guerra fría el FBI, además de la policía francesa y la japonesa trabajaron en el desarrollo de programas algorítmicos que permitieran automatizar la identificación mediante las huellas dactilares. A principios de la década de los setenta, Norman Altman desarrollo y patento el sistema AFIS, o sistema automatizado para la identificación de huellas dactilares.

Otro aporte valioso en las técnicas de identificación fue el estudio desarrollado por Alphonse Bertillon, quien realizo trabajos para aplicar la anatomía en la solución de crímenes. (Peinado, 2018 p 670), Bertillon elaboro las fichas de investigación criminal con su clásica fotografía de frente y perfil más la respectiva medida de altura, brazos, cabeza, orejas, ojos. Para el retrato hablado diseño unos patrones o caracteres físicos los cuales clasifico en; Morfológicos (nariz, boca, orejas, etc.) Cromáticos (color de ojos, bigotes, cabello, barba) Complementarios (talla, grueso, etc.). (Ibídem pág. 671).

Avanzado el siglo XX en el rumor de la guerra fría surgen nuevas formas de captación de datos biométricos como el reconocimiento de la retina, técnica desarrollada por los oftalmólogos Carletto Simon e Isidore Goldstein, obtención que es posible con la lectura de los patrones vasculares de la misma. (Carleto Simón et al.1931)

También se desarrolló el análisis de la voz como dato biométrico, labor que fue posible gracias al trabajo de Lawrence Kersta, físico e ingeniero de los laboratorios Bell, quien invento la máquina espectro-gráfica, elemento que puede grabar sonidos en la forma de gráficos y compararlos después para determinar con un 99% de certeza en su tiempo, a quien pertenece cada voz. (L. Yount 2007 pág., 125). Finalmente el aspecto de más incidencia en los análisis

biométricos, pertenece a la lectura mediante el uso de algoritmos de los patrones que identifican a una persona por su rostro, ojos, labios, cabello, arcos superciliares. Uso que permite estructurar y automatizar el denominado reconocimiento facial, técnica desarrollada a partir de los trabajos de Goldstein et al, en 1972. La tecnología de reconocimiento facial asiente reconocer un rostro o cara en particular dentro de un grupo y realizar contrastes de imágenes, es por esto que hoy este sistema es empleado tanto en verificación como en identificación. Además, las imágenes adquiridas pueden ser en dos claves de datos complementarios; las imágenes de intensidad (estructura de la cara) y las imágenes tridimensionales que compilan la estructura geométrica facial, última que tiene la ventaja de no requerir iluminación ni posición. (Conde Vilda, 2007)

La dificultad en la recolección de datos biométricos es el consentimiento por parte del titular para su obtención, en tal sentido; el acervo de una base de datos de reconocimiento facial no constituye desde este punto de vista una violación a la intimidad o privacidad en el entendido de que esta es elaborada con el previo consentimiento de las personas explicitando detalladamente la finalidad de la utilización de los datos obtenidos (Conde, 2006 p.23).

En la actualidad las tecnologías biométricas más relevantes incluyen; el reconocimiento de huellas dactilares, la geometría de la mano, el reconocimiento de la retina, el reconocimiento del iris, el reconocimiento de la firma escrita, el reconocimiento de la voz y el reconocimiento facial. Último de vital importancia por el desarrollo a partir del convencimiento de que ciertas características del rostro no pueden ser de modo alguna alteradas como son los arcos superciliares, las zonas alrededor de los pómulos, los laterales de la boca, además teniendo en cuenta la facilidad y forma masiva como se obtienen estos datos.

CAPITULO IV

1. Derechos fundamentales y tecnologías biométricas

11.1 Escuchas de voz o interceptación de comunicaciones.

- **Concepto**

En Colombia el decreto 1704 de 2012 define la interceptación de comunicaciones como; **"**Un mecanismo de seguridad pública que busca optimizar la labor de investigación de los delitos que adelantan las autoridades y organismos competentes, en el marco de la Constitución y la Ley".

Se condiciona de esta forma en cabeza del Estado la legalidad en el proceder para las interceptaciones telefónicas o escuchas de voz. A renglón seguido se justifican estas disposiciones con base en el artículo 4, numeral 10, de la Ley 1341 de 2009, la que en desarrollo de los principios constitucionales de intervención, obliga a los operadores de las telecomunicaciones a diseñar, a mantener infraestructuras para el acceso, recopilación de datos o pruebas que sean requeridas por asuntos de seguridad pública, defensa nacional o en casos de emergencia.

Los enunciados anteriores armonizan en su contenido sustancial con los Códigos Penal, de Procedimiento Penal y Penal Militar. Se insta de esta forma a las empresas para que habiliten mecanismos idóneos, con puntos de conexión además de puertos de captura de comunicaciones para tal propósito. Va más allá al imponerles otras obligaciones como su archivo, del mismo modo que la custodia de los datos por un periodo de cinco años. (Artículo 3, ibíd.)

1.1 Marco conceptual

Carl Schmitt definió para su época al Soberano, como aquel que está en capacidad de decidir sobre el estado de excepción, el autor que lo cita propone que si Schmitt hubiese vivido en la época de posguerra posiblemente afirmaría que: "Es soberano quien decide sobre las ondas del espacio". (Byung Chul-Han. ibídem p, 12-13.)

En la Constitución nacional se define al espectro electromagnético como; "un bien público inenajenable e imprescriptible sujeto a la gestión y control del Estado. Se garantiza la igualdad de oportunidades en el acceso a su uso en los términos que fije la ley." (Artículo 75, CN.) Continúa el mismo artículo constitucional indicando que el Estado "solo" podrá intervenir para evitar prácticas de monopolio, proteger la libertad de prensa y la libre competencia económica en el sector. Adicional el artículo 9 del decreto 1900 de 1990, que regula lo concerniente a las actividades y servicios en comunicaciones, delimita la injerencia del Estado a que este debe garantizar; "Como derecho fundamental de la persona la Intimidad individual y familiar contra toda intromisión en ejercicio de actividades de telecomunicaciones que no corresponda al cumplimiento de funciones legales." (Decreto número 1900 de 1990)

En el desarrollo de las telecomunicaciones se han creado escenarios impensados antes para la vulneración de los derechos subjetivos, limitando de manera cierta la libertad y otros valores. La IA ha posibilitado la interceptación de comunicaciones o el ejercicio de labores de vigilancia con una relativa facilidad. Estos actos aparecen justificados por los Estados en asuntos concernientes a su seguridad frente a las posibles amenazas que representan los individuos en determinadas esferas, sea social , político, gremial, pero especialmente con relación a hechos que a manera de terrorismo se han presentado y pueden en lo sucesivo acontecer para afectar la estabilidad democrática, es en este entendido que los Estados a través

de sus agencias de seguridad fortalecen políticas con estrategias diseñadas para combatir el flagelo.

Otra constante para esta vulneración es el ejercicio del poder de determinadas ideologías o grupos políticos. Dispositivos que como mecanismo de detención y afianzamiento del mismo, realizan una coacción sobre sus adversarios políticos que se extiende en general sobre todos los círculos o estamentos sociales, lo anterior tiene un efecto regadera incidiendo de forma indiscriminada e ilegal sobre el total de la comunidad.

Las personas denominadas físicas tienen frente a esto mecanismos de defensa de sus intereses para la protección de la información que les atañe, los datos sensibles solo pueden ser almacenados por los entes gubernamentales en virtud a determinadas excepciones, las personas pueden acceder a sus datos para rectificar o solicitar eliminarlos. En Colombia existen marcos legislativos que lo posibilitan como la ley 1581y otros que en contraste permiten las escuchas de voz.

11.2 Marco jurídico

La interceptación legal de comunicaciones en Colombia se considera constitucionalmente en la Sentencia C-540 de 2012, atinando a que el contenido de la ley 1621 de 2013 como elaboración legislativa para tal propósito, tiene como objeto fortalecer el marco jurídico para las actividades de inteligencia y contrainteligencia del Estado, hecho que implica elementos estructurales básicos que afectan el derecho a la privacidad. En tal sentido se prevee en la visión de la Corte, que las disposiciones de esta Ley estatutaria constituyen un instrumento legal formal que enlaza una tensión limitando el contenido esencial de derechos fundamentales, principios y valores.

El derecho a la intimidad como garantía constitucional en tal contexto se ha definido como:

> "El espacio intangible, inmune a las intromisiones externas, del que se deduce un derecho a no ser forzado a escuchar o a ver lo que no desea escuchar o ver, así como un derecho a no ser escuchado o visto cuando no se desea ser escuchado o visto". (Sentencia C-014/18 14 de marzo de 2018)

Se resalta en tal consideración que el derecho a la intimidad no es de ninguna manera una garantía insoslayable, pudiendo ser limitado para intervenir comunicaciones en eventos en que:

- Medie orden judicial.
- Se presente alguno de los casos establecidos en la Ley.
- Se cumplan las formalidades señaladas en la Ley como en virtud al principio de interés general. (Sentencia C-014/18 14 de marzo de 2018)

Corresponde para el primer evento, exclusivamente al legislador mediante una Ley de tipo estatutaria, ceñido siempre a la observancia, misión y labor objetiva de protección a los derechos humanos constitucionales, así mismo en consonancia con lo dispuesto en los tratados internacionales de derechos humanos y derecho internacional humanitario que los acogen, declarar el ámbito de aplicación de esta Ley u otras similares que lesionen principios y garantías fundamentales, estableciendo en torno un límite al marco legal para su observancia. (Artículo 4, ídem). Continua la corte, para el punto dos, que lo allí dispuesto debe armonizar con lo previsto en los artículos 52 y siguientes de la ley 1453 de 2011, modificatorio del artículo 235, Ley 906 de 2004. Apuntando a que los procedimientos judiciales corresponden muy especialmente a la obtención de pruebas. Articulo 4 y 43, Ley 1621, al lado de otras circunstancias, como la ubicación de imputados, indiciados o condenados, Sentencia C-014/18. Lo que en relación a lo consignado en el artículo 2 del acto legislativo 03 del año 2002, expone que es virtud del criterio exclusivo de las autoridades judiciales competentes en cabeza y a solicitud de la Fiscalía General

de la Nación, CTI, centrales de inteligencia, interferir comunicaciones y poner en práctica procedimientos que afecten a la privacidad, a la intimidad personal o perturben otros derechos fundamentales. En ejercicio de sus funciones la Fiscalía General de la Nación, deberá: Adelantar registros, allanamientos, incautaciones e interceptaciones de comunicaciones. Hechos que de presentarse deberán surtir un control posterior en las 36 horas siguientes por el juez delegado, o sea el juez de control de garantías. La ley 1621 establece en este ámbito como delitos para quienes ejecuten estas conductas, los consagrados en los artículos 269ª, 419, 420, 463, del Código Penal, el 35 del Código de Procedimiento Penal, y los artículos 130 y 131 del Código Penal Militar.

Las acciones de Inteligencia y Contrainteligencia corresponden entonces en la ley 1621; al propósito principal de evitar la comisión de actos terroristas, en tal sentido avanza en un campo más específico como instrumento o marco legal para la captación y tratamiento de datos en cabeza de un responsable; en este caso la policía judicial, a quien se delega también la custodia de la reserva legal definida por la corte como "secreto o confidencialidad" (Artículo 75 CN). En los asuntos de su conocimiento como garantía final a los derechos al debido proceso, a la honra, al buen nombre, a la intimidad personal y familiar, en el entendido de que se les permite conocer a las personas a su solicitud, los procedimientos o acciones que se realizaron o se realizaran en cabeza de los organismos especializados del Estado, debiendo estos indicar los responsables, a quien, como, y en qué periodo se realiza dicho procedimiento. (Artículo 4, ídem.).

De otro lado, la biometría de voz es una de las técnicas más usadas, especialmente en seguridad, debido a su fácil uso e implementación, también por el hecho de que es posible identificar una persona de forma remota, al tener un concepto natural por la tendencia del

humano a expresarse de este modo. (Cesar Tolosa Borja. p.21) Al respecto La ley 1621 de 2013 establece en el segundo párrafo del artículo 17 que:

> "La interceptación de conversaciones privadas telefónicas móviles o fijas, así como de las comunicaciones privadas de datos, deberán someterse a los requisitos establecidos en el artículo 15 de la Constitución y el Código de Procedimiento Penal y sólo podrán llevarse a cabo en el marco de procedimientos judiciales" (Artículo 17, Ley 1621 de 2013).

Dicho lo anterior se hace palpable y manifiesto que cualquier procedimiento o labor para la captación, almacenamiento, además del uso de datos biométricos tipo voz, se ejecutara con el rigor consagrado por la Constitución y los instrumentos internacionales para en tal sentido respetar; La libertad y demás garantías, con el presupuesto obvio de la inviolabilidad consagrada a las comunicaciones privadas.

Cualquier restricción solo puede ser en atención a órdenes emanadas por jueces de la república con el rigor del control judicial sea este previo o posterior, con fundamento en la existencia de un delito o la posible prevención del mismo, para recolectar pruebas o los definidos por la Ley. En relación al control previo también el Juez de control de garantías deberá ejercerlo, sobre las actividades de investigación penal salvo como se ha resaltado en las que afectan a la intimidad con relación al artículo 250 constitucional, cuyo control se realiza con posterioridad dentro de las 36 horas siguientes. (Sentencia C-1092 de 2003). La interceptación de las comunicaciones, según este artículo, solo se materializa cuándo la información recolectada es almacenada en bases de datos. En el entendido de que a tenor de su título la labor especifica de la inteligencia y contrainteligencia se constituye en el monitoreo del espectro electromagnético entendido en este contexto como una:

> "Franja de espacio alrededor de la tierra a través de la cual se desplazan las ondas radioeléctricas que portan diversos mensajes sonoros o visuales. Su importancia reside en ser un bien con aptitud para transportar información e imágenes a corta y larga distancia." (Sentencia C-151 de febrero 24 de 2004)

Se colige entonces en una justa interpretación del artículo que precede, que en Colombia el monitoreo y la vigilancia de las comunicaciones es legal si media orden judicial o lo establecido en la Ley. Según la 1621, no se configura de ningún modo el delito de interceptación por que recae sobre el responsable el deber de secreto profesional al mismo tiempo de reserva legal de la información a la que pueda tener acceso. En este marco, el monitoreo constituye más una labor preventiva ejercida con la finalidad de detectar imágenes, situaciones, afirmaciones o diálogos que pudieran ocasionar circunstancias adversas al interés general, a la seguridad del Estado, de sus instituciones o en previsión de posibles actos de terrorismo. No obstante si se enlaza el monitoreo con el no almacenamiento, en la práctica es una disposición que riñe de bulto con la obligación impuesta a las empresas de telecomunicaciones de almacenar y custodiar los datos por un periodo de cinco años, mucho más al considerar la reserva legal que deberá ejecutarse por un lapso de tiempo de 30 años o para sumar otros 15 en caso de que dicha información trate de la seguridad nacional, pueda afectar las relaciones internacionales, o concierna a grupos al margen de la ley y ponga en peligro la vida de quien esto conoce. (Artículo 33. Ley 1621).

Se evita en tal sentido la consideración de la intimidad como garantía que debe prevalecer sobre el derecho a la información, las empresas de telecomunicaciones pueden cumplir con tal carga, pero se vulnera la intimidad como sustrato que es de la dignidad o elemento esencial de la

personalidad.

- **Vulneración de derechos**

Se reitera con lo anterior que el control jurídico a las labores de inteligencia y contrainteligencia en Colombia ha sido escaso, no existiendo un marco robusto que proteja especialmente al común de los individuos de las intrusiones arbitrarias sobre su intimidad, entendida como; la esfera u orbita privada y reservada a cada persona o individuo ajena a las intervenciones del Estado y otras arbitrarias de la sociedad. De tal modo que le permitan al individuo el óptimo desarrollo de su personalidad y el ejercicio de sus capacidades emocionales, espirituales, culturales con la autonomía de trazar un plan de vida acorde a sus propias características (Sentencia, 2004). La anterior consideración hace parte de las tres formas posibles de violación al derecho a la intimidad en Colombia, a la que se aúnan o se suman: La divulgación de hechos privados, al lado de la afectación a la honra y al buen nombre mediante la exposición tergiversada de hechos o circunstancias personales. (Sentencia T-696 de 1996)

Se puede en tal sentido, comprobar por ser hechos notorios que el Estado colombiano por medio de las agencias de seguridad, ha procedido en interceptar comunicaciones de forma ilegal, arbitraria y consecuente, protagonizando casos de trascendencia pública nacional e internacional. Cabe reseñar que la ley 1621, fue diseñada como paliativo quizás, o como marco legal para suplir las actividades que desarrollaba el extinto DAS (Decreto Ley 4057 de 2011). Por qué; "Se reveló que el DAS extralimitó sus funciones y adelantó seguimientos e interceptaciones irregulares. El escándalo fue conocido como las "chuzadas del DAS", en el cual se hizo cacería a magistrados de las altas cortes, periodistas, sindicalistas, defensores de derechos humanos y políticos de oposición.". (Semana, El Das deja de existir para dar paso a la Agencia Nacional de

Inteligencia, 2011)

Se resalta a lo anterior; la garantía de protección a la privacidad dispuesta en instrumentos internacionales, para que de ningún modo como en el evento considerado por fuera del margen de una labor legal. Persona alguna pueda ser objeto de injerencias arbitrarias en su vida privada, su familia y domicilio, en su Honra o reputación, haciendo un llamado al Estado para que los salvaguarde. (Pacto de San José de Costa Rica Art 11.2)

En tal contexto previamente en el año 2009 la CIDH en comunicado de prensa manifestó su preocupación por la invasión o abuso de las que eran víctimas, individuos de la vida pública y líderes sociales, instando igualmente al Estado para que promoviera sanas prácticas en lo relacionado e instruyera a las agencias estatales que realizaban legalmente dicha labor en la protección de los derechos que con estas actividades resultaran vulnerados, se amonesto a las autoridades, al ordenamiento para sancionar en procesos penal y/o disciplinario a quienes las ejecuten. (CIDH, comunicado de prensa 09/09 de febrero 26 de 2009). Por tales interceptaciones se tienen 20 condenas, que se suman a otras 6 más por el caso de la Central Andrómeda en febrero de 2014, en el que se denuncia la posible reincidencia de ex servidores del DAS quienes a su paso al CTI permitían el funcionamiento de la mencionada "sala gris" en cuyas instalaciones se desarrollaban las interceptaciones.

> "La revista Semana publicó un artículo en el que se denunciaba una Central de Inteligencia Militar encubierta, en donde se estarían también haciendo escuchas ilegales de algunos miembros del proceso de paz con las Farc". (Nacional, 2014)

La respuesta por parte del Estado a manera de sanciones disciplinarias y condenas

penales, además de los informes para aclarar que se hace para proscribir tal práctica vulneradora, ha sido parca y contrario sensu se evidencia en la cotidianidad que estas actividades ilegales se continúan realizando bajo marcos legales que las posibilitan o disponen exabruptos constitucionales, también tramas políticas muy bien elaboradas que evidentemente responden al interés de grupos privilegiados en el poder. A enero del presente (2020) se han evidenciado nuevamente escándalos por "chuzadas" en el ejército, provocando como medida atenuante la salida del Comandante General. Al respecto José Miguel Vivanco (human rights watch) indaga la posible desviación del propósito de algunas ayudas del gobierno de U.S para la lucha contra el narcotráfico hacia esos intereses y hace énfasis en aclarar:

Si estos equipos se han facilitado y el Ejército y las agencias de inteligencia del Ejército los están utilizando para amedrentar, para conseguir información privada de políticos, de periodistas, de defensores de derechos humanos, de la sociedad civil, es un hecho de la mayor gravedad (Vivanco, 2020).

Divulgación de datos

El internet como medio de comunicación masivo tiene para su funcionamiento unos principios que deben observar en el diseño de políticas públicas en atención a la protección de los derechos humanos, estos principios llámese; universalidad, acceso en igualdad de condiciones, pluralismo, no discriminación y la privacidad último que se desarrolla constitucionalmente también en atención al derecho a la libertad de expresión, el acceso a la información y especialmente el aparte del habeas data en el que las personas tienen:

"derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido en bancos de datos o indicado en archivos de entidades públicas y privadas." (Artículo 15, CN)

Los datos como se ha reseñado al inicio tienen además la característica de ser públicos, privados, semiprivados, y sensibles los que como se ha detallado adquieren una relación implícita con el derecho a la intimidad entendida como: "el espacio de la personalidad de los sujetos que no puede ser, salvo a propia elección, de dominio público" (Sentencia T-787 de 2004). Los Estados y cualquier intermediario que con el direccione están en la obligación de proteger a las personas bajo su jurisdicción en su derecho a la privacidad y no esquematizarlos con cualquier tipo de diferencias o ampararse en sus principios para ejercer tal actividad. En Colombia no se da garantía a este aparte del artículo 15 constitucional, menos aun si se armoniza con los artículos 23 y 74 ídem, al no permitir el acceso a los datos que de un particular o persona física se tengan recolectados en bases del ámbito público. Esto cuando de manera voluntaria un usuario consiente el tratamiento sobre los que tiene titularidad en el entendido de que tal autorización se hace con base en unas condiciones que establecen los fines, la duración, con quien y como pueden ser estos compartidos o divulgados.

La ley de transparencia y acceso a la información. (Ley 1712 de 2014). Es el instrumento idóneo a través del cual toda persona puede acceder a los datos de los que es titular en el rango de lo público o de: "Toda información que un sujeto obligado genere, obtenga, adquiera, o controle en calidad de tal" (Lit. b, Articulo 6, Ídem.). No obstante, el mismo instrumento legislativo impone excepciones para atender una solicitud a tenor del título III, y en especial lo dispuesto en los primeros siete literales del artículo 19. Que expresan la excepción o negativa de acceso en virtud al daño a los intereses públicos, esto es, casi las mismas excepciones que pueden invocarse para afectar el derecho a la intimidad, en un proceso. (Tutela, 2018). A saber; cuando medie una orden judicial, cuando sea necesaria para un asunto de esa índole y cuando se afecte la seguridad o defensa nacional, último para cuya articulación cuando el Estado diseñe

estrategias para tal fin, la Corte y los estamentos internacionales se han pronunciado en el entender a estos instrumentos como disposiciones formales que en ningún momento pueden desbalancear los derechos fundamentales otorgados a las personas debiendo respetar las garantías concedidas porque:

"La obligación estatal de asegurar la paz y el orden no permite a las autoridades olvidar su deber de respetar y no vulnerar los derechos humanos, y por ello todas las políticas de seguridad están enmarcadas por el estricto respeto a los límites impuestos por los derechos humanos." (Sentencia C 251, 2002).

Difusión

Las interceptaciones telefónicas en Colombia no son cosa del pasado, se han remozado al calor de las nuevas tecnologías biométricas, la Ley 1621 como propuesta legislativa de contención a esta ilegalidad, realmente puede permitir a estos delitos mudar de piel para adquirir formas más vigorosas de presentación. En el contexto de lo digital un inmenso porcentaje de los datos que se generan son obtenidos en formatos que permiten el uso de tecnología biométrica, estas técnicas consienten la difusión casi que de forma indiscriminada de los datos en poder de una persona obligada. La difusión de la información pública catalogada como de reserva proveniente del monitoreo o vigilancia permitidos por la ley 1621, es posible si se es un destinatario o receptor de este producto (Artículo 36, ídem). Así; El ejecutivo, los secretarios generales, los ministros, los miembros de la fuerza pública según sus funciones o niveles de acceso, también las agencias de inteligencia de otros países con los que se tiene convenio de colaboración, son destinatarios legales.

De igual forma el procedimiento para su difusión debe estar enmarcado en los principios y fines establecidos en el artículo cuarto, en donde cabe resaltar el inciso final que dispone:

"En ningún caso la información de inteligencia y contrainteligencia será recolectada, procesada o diseminada por razones de género, raza, origen nacional o familiar, lengua, religión, opinión política o filosófica, pertenencia a una organización sindical, social o de derechos humanos, o para promover los intereses de cualquier partido o movimiento político o afectar los derechos y garantías de los partidos políticos de oposición" (Ley Estatutaria, 2013).

Se advierte la cercana relación con la definición de datos sensibles desarrollada. Recientemente el país adquirió un software para la vigilancia o el monitoreo denominado hombre invisible, sistema que permite la recolección, reserva, búsqueda de información en el ciberespacio. Estos equipos tenían como potenciales usuarios los batallones Brimi1, Brcim2, destinados a labores de Inteligencia y Contrainteligencia. En este proceso de contratación se detectaron anomalías e incumplimientos consistentes en que:

> "La información alrededor de este proceso licitatorio fue catalogada como ultrasecreta, pues, de conocer algún sospechoso sus detalles serían "posible para un rival generar herramientas para su protección, dejando inservibles los elementos." (Ibídem)

La ley 1712, es clara al solicitar la información mínima, así como la estructura de funcionamiento de los sujetos obligados en las que se incluyan las limitaciones y los deberes de publicidad para las acciones que se ejecutan como son; plan de compras, presupuestos, plazo de cumplimiento de los contratos, informes de gestión y evaluación, políticas adoptadas con sus fundamentos. Eventos en que de evidenciarse inconsistencias puede el contrato ser modificado, además la Ley en que se ampara (1621) ser declarada inexequible por los Congresos acorde con los procedimientos establecidos con anterioridad, o en el evento de no observancia o aplicación

"pueden dar lugar a que se plantee la inconstitucionalidad por omisión," (Valadés, 2020). El uso de los equipos finalmente fue asignado a dos coroneles; uno activo y otro retirado. (Semana Ibídem). Se conoce por las investigaciones de esta revista de que fueron utilizados para actividades políticas y el producto del seguimiento entregado a un reconocido militante de un partido mayoritario.

Las retaliaciones a este medio de información no se hicieron esperar, en año 2019 sus instalaciones fueron asediadas y algunos periodistas víctimas de vigilancia, el más reciente informe de la ONU para este año destaca 113 amenazas, 360 agresiones y dos homicidios contra periodistas en Colombia (A/HRC/43/3Add.3). También tiene apertura por parte de la Fiscalía investigaciones por denuncias y "chuzadas" presentadas por un Gobernador, un Senador del partido de la U, y una Magistrada de la Corte Suprema de Justicia.

En Colombia no se castiga debidamente a las personas obligadas por la firma del acta de compromiso de reserva. (Artículo 38, Ley 1621). Las sanciones por mala conducta y las condenas penales tienen poca efectividad. Consecuencia de esto es la repetición en el tiempo y en los actores de los mismos hechos. A saber; las interceptaciones telefónicas y la consecuente vulneración al derecho a la intimidad. Los funcionarios inescrupulosos que trasgreden con estos delitos, campean en las instituciones, medran en los cargos directivos, ascienden o permanecen en el escalafón.

El Estado o quien debe proceder permite que con estas conductas se lesione además la propia imagen, entendido como ese derecho autónomo que es vulnerado conjuntamente con la honra y el buen nombre de entidades como el Ejército Nacional, (Tutela T-634 de 2013, Colombia). También de las personas honestas a quienes en virtud de tales delitos se les menoscaba en su integridad moral y profesional con imputaciones calumniosas para afectar

igualmente su reputación mediante la divulgación tergiversada de hechos o circunstancias personales, como es el caso del montaje mediático de las chuzadas al general Humberto Guatibonza. (Semana, Otro montaje y una infamia más., 2020). Se asume entonces que cuando se lesiona el derecho a la propia imagen se vulnera paralelamente el derecho a la honra, en cuyo evento no se excluyen la coexistencia de perjuicios para el reclamo de responsabilidad del Estado que se derivan del aspecto psicológico (Sentencia, 2014) con relación al disfrute de bienes y derechos como el libre desarrollo de la personalidad explicado en términos de Gil Colomer como "La facultad natural del hombre para hacer legítimamente lo que conduce a los fines de su vida" (Gil Colomer, R. (2000).

Las interceptaciones telefónicas u otro medio de intromisión en la esfera de la privacidad, hacen nugatorio el disfrute de ese espacio íntimo en el que la persona puede desarrollar sus más profundas convicciones, al sentirse observado además de cohibido para expresar sus sentimientos, en tal sentido la realidad que el individuo quiere aprehender como suya resulta maquillada al ser anulada por circunstancias adversas que le son impuestas desde afuera a manera de coacción al divulgar la información privada que le concierne . Se siente menos capaz de dejar ver caso por caso las facetas no públicas de su personalidad necesarias para fortalecer relaciones personales o sociales, en su gremio por ejemplo vera minada la confianza adecuada para consolidarlas en el afán de gestionar asuntos pensados en proyectos a largo plazo sobre los cuales no podrá llenarse de optimismo para desarrollar sus capacidades y expectativas, no podrá preguntarse de que está en capacidad de realizar sino más bien que le permiten llegar a ser.

En sus relaciones personales se afectara de igual modo la libertad útil para la expresión de sus más intimas motivaciones, que se verán bloqueadas por la falta de sinceridad al no poder construirlas en forma honesta y determinar el camino que más le ayude a crecer para comentar,

compartir, crear, utilizar palabras que le llenen de felicidad. porque estas mismas pueden ser oídas, divulgadas o censuradas remarcando limitaciones para transformar estos sentimientos en relaciones de verdadera, amistad, confianza, amor (Kang, 1998).

14. Reconocimiento Facial

14.1 Definición y concepto

"El Sistema de Reconocimiento Facial es un software automatizado de identificación biométrica capaz de identificar o verificar una persona mediante la comparación y el análisis de modelos basados en sus rasgos y contornos faciales." (Interpol, 2020) Lo anterior implica que para poder comparar y realizar el análisis, la imagen del rostro con sus características transformadas en algoritmo, debe encontrarse almacenada o disponible en forma de plantilla en un sin número de bases de datos. Este dato algorítmico puede de este modo ser cotejado para más certeza con otras plantillas almacenadas, con otras particularidades del cuerpo o diferentes tipos de datos. El reconocimiento facial, es una práctica que permite la extracción de la identidad de una persona de manera univoca.

> "La tecnología de reconocimiento facial es una de las varias tecnologías biométricas que identifican a los individuos midiendo y analizando sus características fisiológicas y/o conductuales." (GAO-15-621. 2015)

El reconocimiento facial en adelante RF, como método de recolección de datos no es de ningún modo la más inofensiva de estas técnicas, en el entendido de que es esencialmente una práctica que no exige ningún tipo de contacto, razón suficiente para que en su implementación los Gobiernos se cercioren para su legal funcionamiento el cumplir con unos parámetros de seguridad y protección a las garantías fundamentales de las personas. Una toma del rostro en un dispositivo con RF, puede proporcionar para el interesado todos los datos que identifiquen a su

titular como; nombre, edad, pertenencia a organizaciones, estado de salud, origen étnico, sexo y posiblemente con los nuevos desarrollos también los rasgos de comportamiento o de conducta del individuo. Conjunto que si son indebidamente tratados enmarcan de forma palmaria una violación a derechos fundamentales e incorporan una intromisión ilegítima en la privacidad.
Los datos biométricos son datos sensibles, los datos sensibles biométricos a diferencia de otros son proporcionados por el propio cuerpo, en los U.S la ley Bipa del Estado de Illinois los define como; "la información personal que puede utilizarse para identificar de manera única a una persona a su cuenta o propiedad." (La ley Bipa no es oponible a Hipaa). Esta Ley trata de asuntos relacionados con la recopilación, uso y almacenamiento de este tipo de datos en el entendido de que esto solo es posible mediante el consentimiento expreso además por escrito del titular, este instrumento tiene campo de aplicación en asuntos comerciales (Ley de Privacidad de la Información Biométrica). Otras excepciones propuestas para el procesamiento de datos con RF, en los lugares y países en donde legalmente funciona, ejemplo Francia, con programas como ALICEM, (Autenticación en línea certificada en dispositivos móviles, 2019), también en los U.S en virtud a la armonización de leyes como la CCPA, exigen la observancia en situaciones puntuales como las definidas en el artículo 9 RGPD, enmarcadas en casos como cuando una persona da su consentimiento, por razones de seguridad nacional o publica, en el ámbito de situaciones legales, además de los datos personales que el interesado ha hecho manifiestamente públicos. (Literal e, Art 9, RGPD)

- **Usos**

En los Estados Unidos como bien se ha indicado, no se tiene una regulación como en Europa que a manera de reglamento pueda aplicarse para esquematizar o acoger el amplio rango de trabajos

que hoy se da a los sistemas biométricos, menos aun cuando se trata del uso de esta tecnología en asuntos de índole comercial, rutina muy extendida en la sociedad norteamericana especialmente como aplicación en la vigilancia. Así el RF es cotidiano como clave de acceso a instalaciones físicas y virtuales, como contraseña de desbloqueo en dispositivos o buscador en redes sociales, para la administración de aeropuertos, escenarios deportivos, en carreteras para la revisión de licencias de conducir, o simplemente en experimentos de impacto social como el realizado por la Universidad de Colorado, que arrojó como resultado que el sistema presenta falencias cuando se trata de la identificación de género al no: "conocer otro idioma que no sea masculino o femenino, por lo que muchas identidades de género es posible que no sean correctas" (Facial recognition software).

Recientemente también se ha implementado su uso en la seguridad para la policía local, estatal, así como para cualquier agencia federal o del Estado como subdivisión política del mismo, un abogado del Gobierno por ejemplo puede solicitar el uso del RF o de registros que estén en una base de datos.

- **El problema**

Los primeros usos diseñados para el reconocimiento facial en U.S, emergen como oportunidad en la verificación de identidades. El desarrollo de las tecnologías en el último lustro, aunado al auge del comercio electrónico con las apps, han re direccionado esta tecnología en temas como la domótica y la cibervigilancia del hogar o comunitaria. En la actualidad de estos sistemas en los U.S el que más ha levantado ampolla por las novedades que pretende integrar es el denominado anillo amazónico, nombrado así por la aplicación "ring" o "vecino" , (Siminoff, 2019) del gigante de ventas online, producto que se integra e involucra en la vigilancia comunal a las agencias de aplicación de la Ley, (Siminoff, 2019), a través de cámaras de seguridad o de video

instaladas a modo de "door view cam", software que puede ejecutar en tiempo real un reconocimiento facial a través del celular. Con este tipo de dispositivos se logra ver, escuchar, y hablar con cualquier persona que se acerque a la propiedad, existen además otras versiones que se integrar a una app que consigue enviar imágenes simultáneas o estar conectados con la policía local o estatal así;

> "Un video puede ser analizado por un dispositivo de grabación y comunicación de A / V que grabó el video (y / o por uno o más servidores de back-end) para determinar si el video contiene un criminal conocido (por ejemplo, delincuente convicto, delincuente sexual, persona en un lista de "más buscados", etc.) o una persona sospechosa". (CNET, 2018).

Las críticas para amazon se concretan en que es su negocio; la vigilancia, allende los marcos legales. Las dirigidas al Gobierno y a las agencias de aplicación de la Ley, están encauzadas por su conexión o connivencia para infiltrar hogares, captar así mismo almacenar datos sin autorización en bases que pueden ser accedidas, entrecruzadas o compartidas de forma anónima por la policía, las agencias y/o terceros no obligados, vulnerando la esfera de la privacidad al mismo tiempo que restringiendo libertades. (CNET, 2018). En el congreso de los U.S, se han manifestado acerca de esta dificultad al lado del despliegue comercial de estas tecnologías. De manera más puntual se tiene la preocupación por su potencial mal uso al ser aplicadas para identificar o rastrear personas en público sin su conocimiento o consentimiento sumado a la posible reserva, mal uso delictivo, e intercambios de información. (Office, 2015).

E instan a formular códigos éticos o manifiestos de voluntad que se hagan exigibles al gremio comercio.

En los U.S la adopción de estos códigos es posible mediante mociones que condicionan,

no aprueban, estableciendo guías para el funcionamiento siempre que se enmarquen en la observancia de principios como los determinados por la sociedad portuaria de Portland (Motion 2019-13, 2019), o en prácticas que en definitiva avocan por un consentimiento de parte del titular de los datos con la revelación por el que lo ejecuta que se está usando y se ha implementado este tipo de tecnología. Además, debe resaltar en sus avisos de que por ningún motivo esta será utilizada para determinar; raza, origen nacional, sexo, color, discapacidad o edad. (An ethical framework for facial recognition, 2014). En tal sentido como ejemplo la Ley de transferencia y responsabilidad del seguro médico Hipaa, contempla las regulaciones observadas anteriormente, también agrega la necesidad de autorización por escrito para el tratamiento de información relacionada a la salud, con las precauciones que debe considerar el autorizado para que pueda revelar información sobre esa persona, además dispone para el evento de datos erróneos en la información, la obligación de notificación para que pueda corregirla, del mismo modo la eliminación de datos o imágenes considerados biométricos antes de su publicación. (GAO, 2016).

14.2 Contexto teórico

El rostro es por esencia un dato público, su captación con el RF, es posible en cualquier sitio abierto haciendo imposible en virtud a esto el anonimato. Cuando se utiliza un sistema de RF, en la actualidad este puede realizarse en 2D o en 3D la diferencia entre ambos estiva en que el primero reconocerá no solo personas físicas y en movimiento como también a una fotografía de su rostro. El procedimiento en 3D está destinado a personas físicas mediante la utilización de luz infrarroja.

Esta tecnología, permite reconocer un rostro o cara en particular dentro de un grupo y realizar contrastes de imágenes, es por esto que hoy este sistema es empleado tanto en verificación como

en identificación. “El reconocimiento facial es el único sistema biométrico que puede emplearse en vigilancia” (Richard Marí Sagarra ediciones UPC 2006). El acervo de una base de datos de reconocimiento facial no constituye desde este punto de vista una violación a la intimidad o privacidad, si es en el entendido de que esta es elaborada con el previo consentimiento de las personas explicitando detalladamente la finalidad de la utilización de los datos obtenidos. (Conde, ídem pág.)

Ninguna ley federal en los U.S regula el uso comercial del RF, mucho menos abordan el problema que se ha planteado en torno a la vulneración de algunos derechos fundamentales y humanos, como es el caso puntual de la privacidad y el libre desarrollo de la personalidad -léase a la propia imagen o en este contexto right of publicy.

- **Usos permitidos**

Aparte de la vigilancia sea esta privada, comercial, o la oficial en sitios públicos, ejemplo carreteras y sitios fronterizos, existe también el uso del sistema de RF, para ser implementado en seguridad por parte de Estado o sus agencias. (Incluyendo la oficina ejecutiva del presidente) En tal sentido el FBI (Federal Bureau of Investigation) hace uso de esta tecnología desde el año 2011, dando inicio al plan piloto denominado NGI-IPS. Para el 2015 el sistema paso la prueba y entro en funcionamiento pleno en el supuesto de ser una tecnología fiable que permite la búsqueda de criminales en bases de datos con más de 30 millones de fotografías. No obstante, como bien ya se ha perfilado en las leyes comerciales, en las guías, o en los acuerdos de voluntades, en todos ellos no se aclara de forma amplia el problema de la privacidad. (Privacy Policy Guidance Memorandum. 2008). Por no tener instrumentos legales que posibiliten la regulación de esta nueva tecnología. Sin embargo, para las agencias federales como es el caso

del FBI, existen marcos legales que regulan el uso de esta clase de métodos en pro de prevenir la posible afectación de los derechos y libertades civiles.

Tal acontece con lo dispuesto por la Ley de Privacidad de 1974, incluida en el código civil de U.S Título cinco, Sección 552a, la cual es posible dique que contiene la recopilación, uso y divulgación de la información o registros depositada en las bases de datos de las agencias del Estado.[1] (Ley de privacidad, 1974).Este instrumento da garantía a un posible control en caso de solicitarlo por parte de un individuo, sobre la información o registros que le pertenecen o han sido recolectados en el sector público. La Ley de privacidad le otorga al individuo tres derechos frente a la acción de las agencias federales, en este caso el FBI, como son:

a) El derecho de cada individuo a ver sus propios documentos, sujetos a las excepciones de la Ley.

Existe la excepción contemplada en el literal j, numerales 1 y 2 que se verifican cuando el registro y recopilación de datos es realizada por la agencia central de inteligencia CIA, o un componente de la misma para ejecutar funciones relevantes en virtud de determinar:

Los antecedentes de delincuentes individualizados o presuntos.

Las investigaciones e informes de informantes que se asocien a esta clase de individuos.

Los informes concernientes a un individuo identificable en cualquier estado o etapa de una investigación penal.

b) El derecho del individuo a corregir su documento, si el registro es incorrecto, irrelevante, inoportuno o incompleto y

c) El derecho a demandar al gobierno por violaciones a la Ley, incluyendo si el gobierno permite a otros ver tu documento personal.” (Ley de privacidad 1974)

Lo dispuesto en los literales anteriores, adolece para las agencias estatales el deber de notificar o publicar avisos a través del sistema SORN (Sistem of Records Notice), cuando se trate del ámbito de aplicación de la Ley de privacidad o en responsabilidades de agencias federales.

En la ley de libertad de la información también se dispone que una organización puede acomodar la eliminación de información personal cuando esta afecta a la privacidad, labor que se realiza mediante el uso o puesta en práctica de mecanismos destinados al usuario a modo de política de uso de datos, para que este pueda solicitar la exclusión o eliminación de los suyos, en el entendido de que la solicitud deberá en cada caso sustentarse necesariamente por escrito. En armonía con las disposiciones anteriores la ley publica E-Government Act of 2002, dispone las situaciones plausibles que deben ser acatadas por los directores de las agencias gubernamentales para los datos sensibles en atención a la protección debida a los derechos fundamentales y a las libertades civiles por lo cual las agencias deberán explicitar:

Qué tipo de información y porque se recoge, que uso que se le dará o con quien se compartirá, lo anterior aunado a los mecanismos que tiene la persona para acceder a la información como a las formas de notificación.

Se ordena además a las agencias el comunicar si esta información "se estaba creando para un sistema de registros con arreglo a la Ley de Privacidad". (Ley Pública 107-347, 2002)

- **Prohibiciones**

El proyecto de ley1215 (AB-1215, 2019) prohíbe el uso de cámaras de RF con conexión a oficiales de la policía durante los procedimientos en el entendido de que: "sería el equivalente funcional de requerir que cada persona muestre una tarjeta de identificación personal con fotografía en todo momento en violación de los derechos constitucionales reconocidos". Se

relaciona esta interpretación al calor de la cuarta enmienda porque que es sustrato de los requisitos para que una persona pueda ser solicitada que medie una disposición u orden legal para proceder a un requerimiento en público. El RF revela necesariamente el dato conexo que no es procedente en un registro habitual, es decir que lo estrictamente privado se eleva a un rango público dando a conocer lo que en rigor debería conservarse entre cuatro paredes o en la intimidad del hogar o gremio.

- **Prohibición de RF en San Francisco.** (Acquisition of Surveillance Technology, 2019) La ordenanza número 190-110 hace relación a la protección de las enmiendas primera, cuarta, décimo cuarta y al artículo 1 de la constitución de California. Prohíbe el uso del RF en los aeropuertos de la cuidad en razón a que históricamente el uso de sistemas de vigilancia masiva está supeditado a la posible orientación de control de las clases menos favorecidas o más vulnerables.

Se expone además que los usos útiles son superados con creces por los riesgos que esta tecnología contiene, mismos que bajo ciertas circunstancias pueden ser asumidos por las agencias o personas que lo soliciten en el entendido de que ciertas disposiciones son taxativas para cumplirlas a cabalidad y en su totalidad como lo son ; que el uso esté justificado por circunstancias exigentes, que la recolección y reserva de datos se realice por un periodo de siete días, conservar solo los estrictamente necesarios, no divulgar a un tercero bajo ninguna circunstancia o solo en caso de ser determinantes para una investigación judicial o esclarecimiento de un delito, presentar informe escrito que defina el equipo utilizado y sus características para la captación. (Ordenanza, 2019)

- **Prohibición en Somerville**

Este condado de Massachusetts, Pone en consideración de que no habrá ningún sistema de recopilación de datos de RF en su jurisdicción o territorio, de modo que en el evento de presentarse datos en procesos o como evidencia probatoria que tengan origen o sustrato en esta tecnología, serán considerados como documentos ilegales y eliminados sin oportunidad de descubrimiento.

- Prohibición en Oakland (Código Municipal de Oakland, capitulo 9.64)

En el análisis para proyectar la ordenanza de prohibición del RF en esta ciudad, se enfatiza que este tipo de tecnologías hace a la comunidad mucho más insegura por el temor de muchas personas a testificar en eventos donde se tenga el RF como prueba, esto debido a la maleabilidad de la tecnología por la aprensión a incurrir en falsas apreciaciones o por ser evidentemente proclive a sesgos discriminatorios, condiciones que pueden ser la causa de encarcelamientos injustos, deportaciones, revelación de hechos, gastos innecesarios a la administración pública y la persecución basada en minorías. Esta ordenanza se acompaña de un detallado informe denominado Sombras de Género: Disparidades de Precisión Intersectorial en la Clasificación de Género Comercial (Buolamwini, 2013). En el que en síntesis se observa que algunas agencias estatales al utilizar las bases de datos de RF, han procesado informes basura en los que se comprueban casos de falsos positivos determinados por el color de la piel o por el género de las personas. Los datos muestran que esta tecnología identifica de manera negativa y desproporcionada a las mujeres de piel oscura y en otros casos se afirma que se arrojaban datos erróneos sobre un individuo y para suplir este error su fotografía es reemplazada por la de alguna celebridad. Sobre la eficacia del sistema de RF el director de la Oficina Federal de investigaciones ha sido enfático en las mejoras que aún les faltan a los algoritmos. Es igualmente consiente de que se adolece de normas que regulen su uso, a lo cual expresamente afirma que:

"En la ausencia de normas, una moratoria sobre el uso del RF a nivel local, estatal y federal es apropiada y necesaria" (Ídem pág. 29.)

- **Prohibición en Cambrigde** (Orden policial número 255 de enero 13 de 2020)

"El uso de la tecnología de reconocimiento facial puede tener un efecto escalofriante en el ejercicio de la libertad de expresión protegida constitucionalmente". La libertad de expresión no solo incluye su manifestación directa, porque están contempladas también las expresiones indirectas que se enuncian a través de actos o mensajes simbólicos, como son prendas, pancartas, banderas. Esto porque se afirma el uso del RF, en manifestaciones pacíficas por la muerte del joven negro Freddie Grey, por lo que las personas serian accedidas en sus datos y estos almacenados para su identificación o contraste relacionándolos con este tipo de manifestaciones o actividades.

- **Derechos vulnerados.**

El los U.S el derecho a la privacidad se ha configurado desde la doctrina y a través de la jurisprudencia, no existiendo propiamente en la Constitución una designación expresa, pues se ha construido mediante la interpretación de enmiendas fundamentalmente la primera, la cuarta y la decimocuarta. Última de especial apreciación por hacer referencia a la libertad de elección individual como núcleo intangible de su protección derivada del debido proceso legal sustantivo.

Sin embargo, en donde realmente puede verse plasmado de forma notoria el derecho a la privacidad en los U.S, es en la protección de la denominada información personal. Regulada en disposiciones contenidas en la Ley de privacidad de 1974 y en la Ley publica 107-347 de 2002. Jurisprudencialmente se han considerado tres eventos o presencia de intereses que se pueden

apelar en la demanda para la protección del derecho a la privacidad o información personal como lo son:

El interés individual en evitar la divulgación de asuntos personales.

El interés en la independencia para tomar ciertas clases de decisiones importantes y libres de la compulsión gubernamental.

Finalmente el derecho del individuo a ser libre de la vigilancia e intrusión gubernamental en sus asuntos privados. (Whalen v. Roe, nota 24)

- **Ser libre de la vigilancia e intrusión gubernamental en sus asuntos privados**

"El derecho a ser dejado solo, a vivir la vida que uno elige, libre de agresión intrusión o invasión, a excepción de las que puedan estar justificadas por las necesidades claras de la vida en comunidad bajo un gobierno de leyes". La anterior disposición señala el límite entre lo público y lo privado, la captación de la imagen en espacios abiertos posiblemente genera para el Estado, un amplio campo de confort en el cual es soberano. Pero allí emerge la dificultad de definir el espacio de lo privado porque entraña además el concepto o derecho de la propiedad, la esfera privada del individuo incluye su hogar y su familia , también el gremio en el cual mantiene sus negocios, en este espacio es inmune a las invasiones arbitrarias, cada hogar es para quien un castillo de fortaleza invulnerable aún frente al Estado o sus agentes, al trascender al contexto público con técnicas de RF los datos sensibles pueden perder ese valor ante el Estado o menguar en su disfrute por ser entregados inermes a la vulneración justificada en pro del interés general, la defensa o seguridad, situaciones que en múltiples eventos no son justas causas o procedimiento legal para acceder a los datos de una persona, menos aún almacenarlos indiscriminadamente sin realizar distinción entre datos comunes y datos sensibles, los que aún en

el ámbito de lo público continúan en cabeza del individuo afectado como su titular frente al Estado para acceder a los mecanismos o ejercer las acciones procedentes para su protección o su eliminación de las bases de datos si así lo requiere.“No podrá Estado alguno privar a cualquier persona de la vida, libertad o propiedad sin el debido proceso legal” (Enmienda XIV, 1868).

- **Divulgación**

La tecnología de RF realiza captaciones de datos personales y sensibles de forma indiscriminada, un programa como el ring de amazon y su aplicativo vecino, pueden interrelacionarse con las agencias de aplicación de la ley para compartir datos al mismo tiempo que se “generan conversaciones sobre el crimen en las comunidades” (Ring.), para el corriente 405 agencias locales están integradas a través de dispositivos en los que los usuarios publican indiscriminadamente la información que consideran importante para su seguridad, así en el supuesto de que alguna persona haya quedado evidenciada en el radio de captación de su lente o en lo que consideran la esfera de su privacidad puede ser catalogada como sospechosa y difundida como tal.

Los vecinos, las agencias locales, podrán de esta forma ver además de comentar la información o pedir ayuda mediante la presentación del video obtenido con el dispositivo. (Ring, 2020). Por disposición legal las agencias del estado solo pueden acceder a los datos de personas indiciadas, en flagrancia, para resolver delitos o de que medie una orden judicial. La ley de privacidad protege la información personal controlada por estas así mismo regula la forma en que el gobierno a través de sus agencias la pueden divulgar o proveer acceso. (Ley de privacidad, 1974)

Si la captación se realiza de forma masiva e indiscriminada sobre las personas e individuos que se acerquen a la cámara, surge entonces el interrogante de como la Corte puede interpretar la cuarta enmienda, en el entendido de que esta, en su esencia protege contra búsquedas injustificadas y en este caso la autorización para hacerlo, como se ha indicado demanda que se justifique la causa en que se procede y la individualización de a quién o porque se le está realizando.

En el contexto de lo público y de la información que allí este depositada, se exige la transparencia como contraparte o como protección de la privacidad en el entendido de que no es solo comunicar la información que sobre un individuo se dispone, si no del control que la persona tiene sobre esto, para negar o conceder el acceso a otros. Los datos biométricos son datos sensibles y su difusión está prohibida sin que medie consentimiento o disposición legal para ello.

Muchos datos pueden ser de dominio público como el nombre, identificación, el género, pero en el campo de los sensibles cuando se hace sin consentimiento se vulnera la dignidad. La privacidad es la exclusión del otro del conocimiento sobre uno mismo si tal se procede se afecta la esfera íntima de los sentimientos y sensaciones.

La captación de datos con dispositivos de RF vulnera la primera enmienda “Libertad de culto, de expresión, de prensa, petición, y de reunión”. (Enmiendas a la Constitución de los Estados Unidos de América). El derecho a la propia imagen ha correspondido en esta legislación con el derecho a la libertad de información y de expresión. Porque la propia imagen o the right of publicy como es designado en el derecho anglosajón se asume patrimonialmente como la facultad de explotarla, reproducirla, exponerla, y publicarla. Pero lo que entraña la garantía de este derecho en este ordenamiento es la imposición de la potestad en cabeza del titular de

difundirla (Humberto Nogueira Alcalá.) y de allí su estrecha relación con el derecho al libre desarrollo de la personalidad.

La captación permanente e indiscriminada de datos a través de la vigilancia con RF, coarta la Libertad, a la que Rawls resalta como "un complejo de derechos y deberes definidos por las instituciones" (Citado en La noción de libertad en John Rawls, Carlos Massini Correas).

El Gobierno como institución puede limitar la libertad de expresión amparado en una justa causa, como lo es la seguridad nacional, pero no podrá hacerlo en virtud a la simple manifestación de expresión, porque sería un sesgo discriminatorio que atenta contra la justicia y la posibilidad de que los individuos se realicen en su proyecto vital: “Esta tecnología permite rastrear a las personas sin su consentimiento. También generaría bases de datos masivas sobre californianos respetuosos de la ley, y podría enfriar el ejercicio de la libertad de expresión en lugares públicos.” (San Francisco Privacy Ordinance)

Se entendería en tal contexto a la libertad como un derecho condicionado, en donde el individuo sabe de qué la goza física, pero todos los actos de expresión de su personalidad están baldados por la agobiante sensación de monitoreo o vigilancia permanente.

- **La independencia para tomar ciertas clases de decisiones importantes y libres de la compulsión gubernamental**

La libertad negativa relacionada al monitoreo y vigilancia, está vinculada a procrastinar el ejercicio de la autonomía en los individuos, pues esta no brota en ellos por generación espontánea al estar ligada o ser el producto de un proceso continuo. La autonomía implica ser independiente pero dentro de una sociedad regida por unos derechos y deberes, ser autónomo es

apartarse de esta en su conjunto, para elegir como disfruto de mis derechos y ejerzo mis deberes sin más limitantes que la dignidad humana. (Configuring the Networked Self, 2012, Julie E. Cohen). Puedo por ejemplo elegir a mis gobernantes, desplazarme en paz sin ser interpelado, asistir a eventos, compartir con quien guste, de igual modo soy autónomo en mis intimas decisiones, en las que me afecten o beneficien. La «zona de privacidad» protegida constitucionalmente no sólo ampara esa autonomía individual en la toma de decisiones importantes sino también el «interés» individual en evitar la revelación de asuntos personales" (Whalen v. Roe, 429 U.S. 589, 599-600, 605. 1977). Son decisiones importantes entre muchas; el matrimonio, la autonomía religiosa, los asuntos de salud y allí situaciones sensibles como el trasplante de órganos, la autonomía reproductiva, las trasfusiones sanguíneas, el consentimiento informado para la eutanasia, una enfermedad vergonzosa. Son estos últimos además datos sensibles que al ser conocidos por otros sin consentimiento afectan y confinan la privacidad.
El problema en síntesis no reside solo en la captación de la imagen, su transformación en logaritmo para ser almacenado, si no en el acceso a los datos conexos que en esta tecnología está implícito y con esto el control posterior del Estado sobre la voluntad del individuo la que se reitera no tiene más límite que la dignidad.

10. Conclusión

La humanidad ha trascendido etapas irreversibles, la consolidación de la IA es la última de ellas, se manifiesta y presenta como una deshumanización del individuo, en un exceso de información en que todo es conocido, visible, transparente, aún la postrer chispa de la privacidad en el hogar está siendo vulnerada por la tecnología con sus artefactos que captan datos en múltiples formas y dispositivos. Más no todo debería ser del publico conocimiento, al Estado correspondería respetar este sacro lugar de recogimiento individual, familiar y social con lo que allí acontece evidenciado como información en los denominados datos sensibles o definidos como aquellas situaciones particulares a veces incomodas aún para el propio sujeto que al estar imbricadas en lo más profundo de los sentimientos y actividades que solo al titular conciernen pertenecen por tanto a su núcleo esencial de intimidad.

Los datos sensibles corresponden en cada legislación a la categoría de información acreedora de un especial trato y cuidado, la que debe ser preservada de su conocimiento a los demás. Legislativamente se han diseñado instrumentos que atiendan a su protección de tal modo se tienen herramientas de alcance continental como es el caso de RGPD en el que se integran de igual modo para su observación los denominados datos biométricos. Asimismo otros ordenamientos jurídicos se han armonizado con la medida, en Colombia esta dispuesta en la ley 1581 en la cual a tenor de lo anterior también se han constituido la jurisprudencia para la protección de los datos relativos a la pertenencia a organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o garanticen los derechos y garantías de partidos políticos de oposición.

En los U.S la legislación relativa a la protección de datos sensibles es mucho más laxa y permisiva, no se tienen instrumentos de tipo estatutario remitiéndose a mecanismos como los acuerdos de voluntades, la autorregulación, las certificaciones. En salud no obstante si existen instrumentos idóneos de amparo a estos datos como acontece con la ley Hipaa, al lado últimamente se están integrando las disposiciones del RGPD en leyes estatales como la CCPA. Como rasgo distintivo para los datos sensibles se aprecia en todas estas legislaciones el requisito del consentimiento expreso para acceder a la información, todo esto al calor de la protección relativa a la privacidad e intimidad.

La propuesta de privacidad y su camino hacia su consolidación como derecho fundamental se cimienta en la noción occidental de individuo con su voluntad de ser dejado solo en los asuntos que le pertenecen, concepto que además tiene fundamento en los principios de autonomía y libertad sin más limitantes que la dignidad en las personas. Su pasaje se inicia en la doctrina americana con punto de partida en el escrito de Warren y Brandies en 1890, complementándose posterior y paulatinamente a través de la jurisprudencia. En donde puede sintetizarse como: “El derecho a ser dejado solo, a vivir la vida que uno elige, libre de agresión intrusión o invasión, a excepción de las que puedan estar justificadas por las necesidades claras de la vida en comunidad bajo un gobierno de leyes”. Su consideración en otros ordenamientos también está marcada por este rumbo no obstante en el derecho continental y en Colombia se emplea el término intimidad que se asume como un derecho Constitucional fundamental con cimiento en la dignidad humana, que manifiesta su interés y resalta los asuntos relativos al cuerpo de la persona, al desarrollo de la personalidad con los eventos que a este conciernen como son las sensaciones, emociones o sentimientos del ser humano.

De otro lado el derecho a la propia imagen es en Colombia una garantía fundamental de tipo casuístico y debe demostrar el apelante el tipo de daño moral sufrido para obtener resarcimiento. En los U.S es de categoría netamente patrimonial, atiende a la denominación de right of publicy y está dirigido a la calidad e importancia de la persona en que la imagen es afectada.

Las tecnologías biométricas suponen un escenario escalofriante para la privacidad de las personas, los colectivos y las jurisdicciones que se oponen basan sus apuestas no solo en pedir la moratoria mientras se realiza una legislación que la regule, sino en su prohibición de manera total en el entendido de que es una arma de control tan nefasta como lo son las biológicas que deshumanizan el ser humano haciéndolo previsible, plano, mensurable, inerme al control que de él quieran hacer los Estados y quien tenga el poder de almacenar o de analizar estos datos. Además, esta tecnología se supone falible, proclive al robo, al hackeo, es altamente discriminatoria, sesgada y como se ha demostrado con afinidad por un determinado tipo de raza pudiendo así ser usada en detrimento de los grupos sociales más vulnerables. Hoy los Estados se justifican en principios como el de interés general y para muchos en la actualidad la seguridad es el leitmotiv para proceder con la vigilancia o el monitoreo, especialmente a partir del 09/11, los gobiernos se enfrentan cara a cara con sus propios demonios, el ascenso de doctrinas populistas, la lucha por el poder y los recursos, el control de las economías y la contención de los flujos migratorios han facilitado aún en la más robusta democracia el ejercicio paralizante de estas prácticas, (Dockendorff, 2013) . Esto cuando no se refiere a las pugnas intestinas en las democracias menos fuertes de los grupos de poder o partidos políticos que organizan una labor nefasta en su beneficio y que tiene como producto la recopilación masiva de datos, los falsos positivos, la vulneración de derechos fundamentales. La biometría tiene un amplio trasegar como técnica de control así desde las antiguas practicas marcarias hasta los sistemas de control tipo

panóptico y el desarrollo de tecnologías digitales que van dejando atrás los sistemas análogos que presumen un mayor control de la información, para acoger con beneplácito y de manera vertiginosa prácticas que desbordan el control humano, la IA contribuye de esta forma al reemplazo de la razón por previsiones y análisis basados en números o datos. Finalmente se debe poner sobre el tapete de que también es una sumisión consciente y voluntaria de los individuos al ceder su libertad a cambio de una interacción constante, el ciudadano digital en estas labores debe poder resignarse en todo momento a dejar no solo sus datos si no también parte de su personalidad al acceder a un sistema inteligente. Y los Estados previsivos han vislumbrado esta inmensa oportunidad de control y hacia esta apuntan de manera definitiva e irreversible. En Colombia se realiza un tratamiento indebido de los datos personales sensibles a cargo de algunas agencias de seguridad que contrariando las disposiciones legales realizan una labor de monitoreo o vigilancia sobre determinados grupos de personas con el propósito de extraer información que pueda ser usada con fines de control especialmente político. Se vulneran de esta forma los derechos a la intimidad, a la privacidad y a la imagen con el subsidiario desarrollo de la personalidad. Igual desmedro a estas garantías acontece en los U.S con el notable aumento de la tecnología biométrica de reconocimiento facial, auge que ha permitido una complicidad entre un sector del comercio y las agencias de aplicación de la ley, esta práctica se ha considerado en las prohibiciones como muy grave porque aparte de violentar las enmiendas constituye un trabajo constante de cosificación del ser humano.

Para cerrar puede decirse que las tecnologías biométricas tienen amplia ventaja de desarrollo frente a una legislación que las regule, la cual es escasa y en eventos como el RF inexistente.

11. Referencias bibliográficas

Ángel (2012) *"La monografía jurídica"* Elementos fundamentales de la hermenéutica jurídica∗ tesis de maestría página 25

Altuna Lizaso (2011). *Una historia moral del rostro*. Valencia. pre-textos, 297, Physiognomonia (pág. 23)

Artículo 3 de la Ley 1581 de 2012.

Bentham, ídem pág. 84 y ss.

Borja (2019). *Sistemas Biométricos.* Recuperado de: https://www.dsi.uclm.es/personal/MiguelFGraciani/mikicurri/Docencia/Bioinformatica/web_BIO/Documentacion/Trabajos/Biometria/Trabajo%20Biometria.pdf

Carlos Sabino. *El proceso de Investigación,* Buenos Aires. Lumen-Humanitas, 1996, pp 62 y ss.

Conferencia Internacional 2009. *La Declaración de la Sociedad Civil Madrid*, España 3 de noviembre de 2009. Disponible en; https://edps.europa.eu/sites/edp/files/publication/09-11-03_madrid_privacy_declaration_es.pdf Visitado diciembre 20 de 2019.

Consejo de Derechos Humanos en; https://www.ohchr.org/Documents/AboutUs/CivilSociety/Chapter_5_sp.pdf recuperado 17 diciembre de 2019.

Colombia, Ley 1712 de 2014. *Por medio de la cual se crea la ley de transparencia y del derecho de Acceso a la información Pública Nacional y se dictan otras disposiciones.* 06 de mar, 2014 Núm. 49084. Recuperado de: http://www.secretariasenado.gov.co/senado/basedoc/ley_1712_2014.html

Colombia, Ley 1474 de 2011, *por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública*. 12 de julio, 2011 Núm. 48128.

Colombia, Ley 1581 de 2012, *por la cual se dictan disposiciones generales para la protección de datos personales*. 17 de Octubre, 2012 Núm. 48587.

Colombia, Ley 079 de 1993, *por la cual se regula la realización de los Censos de población y vivienda.*20 de Octubre 1993. Núm. 41083.

Convenio 108 del *Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal*. Estrasburgo 28 de enero de 1981. p, 10.

Convenio para la Protección de los *Derechos Humanos y de las Libertades Fundamentales*, Hecho en Roma el 4 de noviembre de 1950.Publicado en España el 10 de octubre de 1979. *Boletín Oficial del Estado Número 243*, 10 de octubre de 1979. Art 8.

Corte Constitucional. Jueves, 16 de octubre de 2008, M.P: Jaime Córdoba Triviño, Sentencia C-1011 de 2008, Colombia.

Corte Constitucional. Sábado, 01 de enero de 2011, M.P: Jorge Ignacio Pretelt Chaljub, Sentencia C-748 de 2011, Colombia.

Deleuze, G. (1999), "*Posdata sobre las sociedades de control",* en: El lenguaje libertario. Antología del pensamiento anarquista contemporáneo, Buenos Aires, Altamira.

En el enjambre, Byung-Chul Han. 2014, Barcelona, Herder. PP. 3-86.

Foucault, Michel, (2015). Vigilar y castigar. Siglo XXI.p. 234.

Ley 1712 de 2014 literal b), articulo 6, Ídem.

Ley Orgánica 3/2018, de 5 de diciembre, *de Protección de Datos Personales y garantía de los derechos digitales.*

Literal e), del articulo 3 ley 1581 de 2012. "*responsable del Tratamiento: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos*".

Manuel Cruz Ortiz de Landázuri. *De la Biopoliticas a la Psicopolíticas en el pensamiento social de Byung-Chul Ha*n Recuperado en: https://atheneadigital.net/article/view/v17-n1-cruz/1782-pdf-es visitado el 17-12-2019

Michel Foucault. (1972-1973). *La sociedad Punitiva.* Curso en el College de France (1972-1973). Ciudad Autónoma de Buenos Aires. Fondo de Cultura Económica 2016, p, 25.

Orden policial número 255 de enero 13 de 2020, disponible en: https://cambridgema.iqm2.com/Citizens/Detail_LegiFile.aspx?Frame=&MeetingID=2399&MediaPosition=&ID=9847&CssClass . visitado febrero 05 de 2020.

Real academia de la lengua en: https://dle.rae.es/sensible

Sentencia T-364/18 *Corte Constitucional Magistrado Ponente*: Alberto Rojas Ríos

Sentencia 94/1998, de 4 de mayo. *Recurso de amparo 840/1995*. Tribunal Constitucional.

Zweigert, Konrad y Kotz, Hein, *Introducción al derecho comparado*, 3a. ed., México, Oxford University Press, 2002, p. 17