**UNIVERSIDAD DE CHILE**
**INSTITUTO DE COMUNICACIÓN E IMAGEN**
**ESCUELA DE POSGRADO**

# AGENDA DE LA PRENSA ESCRITA DIGITAL RESPECTO A LOS TEMAS DE LA PRIVACIDAD DE LA CIUDADANÍA Y LA VIGILANCIA ESTATAL EN COLOMBIA DURANTE EL PERÍODO 2015-2016:
## Sistemas de vigilancia estatal y el caso Hacking Team

**Tesis para optar al grado de Magíster en Comunicación Social**

**IVÁN LEONARDO VALDERRAMA ESPEJO**

**Profesora guía: María Cecilia Bravo**

**Santiago de Chile**
**2018**

*Por la experiencia y el conocimiento de lo importante, gracias a mi familia*

*Por el paso, gracias a Chile*

# TABLA DE CONTENIDOS

**RESUMEN**

El presente escrito pretende describir y analizar la agenda de la prensa escrita digital respecto a los temas de la privacidad de la ciudadanía y la vigilancia estatal en Colombia durante el periodo 2015-2016, valiéndose de herramientas propias del análisis de contenido y discurso para develar el tratamiento editorial que la prensa con mayor lectura en Colombia ("El Tiempo" y "El Espectador") hace de los temas en mención en un momento histórico particular de la nación con las negociaciones de paz entre el Gobierno Nacional y las Fuerzas Armadas Revolucionarias de Colombia – Ejército del Pueblo (FARC-EP).

Se encuentra que, primero, sí existe una agenda respecto a los temas tratados, con mayor cobertura y tratamiento desde El Espectador que desde El Tiempo. En esta agenda se destaca el esfuerzo por dejar un historial de lo ocurrido con los escándalos de los sistemas de vigilancia estatal en Colombia y el mundo, demarcando los efectos a los que se someten tanto los Estados como la ciudadanía en materia de derechos humanos, tecnologías de información y comunicación, y transparencia en la contratación pública.

Se considera que este trabajo cumple con un múltiple propósito tanto para la academia como para el periodista o escritor que trabaja para los medios: por un lado, se obtiene evidencia de las temáticas tratadas y posteriormente, si se desea, profundizar en su tratamiento y acercamiento; por otro lado, puede constituirse en un suplemento adicional para encontrar nuevas categorías de estudio enmarcadas en las categorías 'privacidad' y 'vigilancia'; por último, sirve como medio de denuncia de carácter ciudadano de determinados hechos, en la búsqueda de la defensa plena de los derechos humanos que encubren a las personas para su desarrollo en una sociedad democrática.

# CAPÍTULO I. EL PROBLEMA DE INVESTIGACIÓN

## 1.1. Antecedentes

### 1.1.1. Vigilancia y privacidad en el entorno de las TIC's

La constante preocupación por la seguridad en la sociedad occidental se fundamenta en mensajes de los medios de comunicación masiva sobre delincuencia, asesinatos, terrorismo, ataques cibernéticos, entre otros, que se disponen finalmente en una agenda pública accesible a todo el mundo y que goza de una discusión desde la sociedad y sus instituciones.

El desarrollo tecnológico en los últimos dos siglos ha sido uno de los principales motores de los modelos de producción moderna que en síntesis ha posibilitado la llegada de la sociedad a una etapa tecno-económica conocida como capitalismo informacional (Mason, 2016; Pérez, 2012), caracterizada por tener como inicio y base tecnológica la digitalización de los procesos humanos y laborales, representados en un inicio por las grandes computadoras hasta llegar a sofisticadas máquinas de procesamiento masivo de datos que pueden simular con mayor precisión los entornos individuales y societales.

La seguridad es una prioridad política en la gran mayoría de países a nivel internacional, la cual activa las iniciativas y proyectos propios de un mundo de vigilancia (Bauman & Lyon, 2013), el cual es posible no únicamente a partir de recursos humanos que se disponen estratégicamente en diversas zonas para enfrentarla y/o abatirla, sino también a partir de tecnologías de diferente índole; estas tecnologías son reconocidas hoy fácilmente en diferentes espacios de cotidianidad, como las cámaras que se encuentran en la infraestructura de los edificios y hogares, así como los desarrollos biométricos que permiten el acceso a determinados espacios.

Esta frecuente presencia de tecnologías de vigilancia ha permitido configurarlas dentro de la normalidad de la sociedad como justificación de la seguridad, siendo la implementación de dichas herramientas transformada en una necesidad; las tecnologías de vigilancia deben ser entendidas como el resultado de una configuración social y política relacionada al riesgo y la incertidumbre, configurando una realidad sostenible en el tiempo alrededor del sentimiento de inseguridad (Bauman & Lyon, 2013).

En el contexto de una sociedad-red (Castells, 1999), que cuenta con una infraestructura establecida y robusta como lo es Internet, la comunicación ha gozado de una extensión en su producción y reproducción, que ha resultado en una explosión de información y de interacciones entre seres humanos y [entre] máquinas. Esta forma de ver un mundo digitalizado, como apuntan Bauman y Lyon (2013), es justificado discutiblemente como uno de los mejores mundos para la democracia, las empresas, el entretenimiento y la seguridad, y que Vincent Mosco lo encontró como un espacio mítico que trasciende tiempo, espacio y política, llamándole lo "sublime digital".

Poco a poco, los desarrollos de las tecnologías de información y comunicación (TIC's) han permitido hablar de una esfera digital que hace parte conexa a la vida del día a día que se tiene desde tiempos remotos en la humanidad. Las TIC's no sólo son herramientas (*hardware*), junto a estas vienen desarrollos de *software* de gran envergadura que permiten abordar variados aspectos y necesidades de los seres humanos en el entorno terrenal.

La sociedad-red hoy es una realidad, contando con incontables cantidades de servicios y productos usados por las personas para apoyar diferentes ámbitos de la vida, entre estos, la comunicación. Esta sociedad tiene como uno de sus principales motores la innovación, la que conlleva a indicadores relacionados con el crecimiento económico y cambios financieramente benéficos, escondiendo o

dejando en un segundo plano todas aquellas innovaciones que no salieron como se esperaba o que contaban con una segunda intención (Sveiby, Gripenberg, & Segercrantz, 2012).

Es así que en esta red, a través de las TIC's, hoy es posible monitorear, interceptar, coleccionar, categorizar y preservar datos e información que se transmiten por diferentes protocolos a través del mundo en un constante flujo de códigos a través de lenguaje binario (Mayer-Schonberger & Cukier, 2013). Esta posibilidad de seguir rastros de información ha generado una nueva entrada a la vigilancia en la actualidad, en la que datos-información resultan elementos volátiles pero de gran importancia para la existencia de las TIC's y su desarrollo de gran envergadura.

En esta realidad de vigilancia, es menester hablar de privacidad siendo este concepto uno de sus aliados teóricos: no es posible hablar de vigilancia sin tratar el tema de privacidad, y viceversa. Los alcances de las tecnologías que robustecen los sistemas de vigilancia de la actualidad son cada vez más efectivos, dejando en duda la privacidad de las personas que son sujetos de sus lentes físicos y digitales (Kerr & Barrigar, 2012).

La privacidad ha sido tema de atención para la academia y la agenda pública desde hace tiempo, sin embargo, en la era moderna la concepción se ha encontrado en un límite difuso con lo público (Habermas, 1997), transformándose continuamente; en la última década este comportamiento no ha cambiado, y son las TIC's que influyen y las decisiones que se toman respecto a sus posibilidades. De los avances que han tenido las TIC's en el tratamiento de grandes cantidades de datos han sacado provecho el sector mercantil con el fin de ofrecer servicios y productos personalizados o perfilados con base a los datos generados por las personas en su paso por Internet y, en definitiva, generar ganancias a partir de esto; y los Estados nacionales con el fin de realizar un rastreo del comportamiento de los ciudadanos como medida de prevención a posibles actos delictivos (Fuchs, 2014).

Se puede afirmar que el espacio de la privacidad es cada vez más complejo con los alcances de rastreo e identificación de los sujetos en Internet en función de la seguridad y la vigilancia (Kerr & Barrigar, 2012). Una realidad de vigilancia somete a la privacidad a un replanteamiento no desconocido para su historia, pero sí exigente en tanto se depende de una tecnología que se desarrolla segundo a segundo y que pone en evidencia la fragilidad de su prevalencia en la sociedad y la necesidad de justificar su existencia en la Declaración Universal de los Derechos Humanos.

### 1.1.2. La agenda de los medios y la opinión pública

Reconociendo la influencia de los medios de comunicación en las esferas públicas y, por ende, en las opiniones públicas, en los cuales "se hace y rehace la cultura de las mayorías" (Cogo, 2011) citando a Martín Barbero (2005), la agenda de dichos medios representa una importancia para la representación de la realidad que hacen las personas-ciudadanas de los temas que se difunden y tratan periodísticamente. Es cierto que los medios de comunicación tienen dentro de su agenda los temas de vigilancia y de privacidad de la ciudadanía, más teniendo en cuenta que en la última década los devenires tecnológicos han posibilitado que la realidad de la vigilancia sea aún más visible poniendo en debate la posibilidad de una privacidad integral. Sin embargo, los estudios sobre medios y su tratamiento sobre los temas en cuestión son reducidos y propone una oportunidad y visión relevante de mostrar una realidad que se complejiza social y políticamente, y que al mismo tiempo se avanza en su entendimiento.

## 1.2. Delimitación del problema de investigación

### 1.2.1. Agenda de los medios sobre temas de privacidad de la ciudadanía y vigilancia estatal

Si bien los estudios sobre vigilancia y privacidad de la ciudadanía pueden tener acercamientos interdisciplinarios que puedan explicarlos como un fenómeno dentro de la sociedad, es aún un área del conocimiento en crecimiento que ha llamado la atención de la academia. Al hablar tanto de vigilancia como privacidad se está hablando de dos conceptos que se encuentran en un área gris cuando de asumir una posición al respecto se habla, es decir, cuando se tratan estos conceptos se asume una posición en la que se ubica una por encima de la otra, en la que el nivelarlas resulta a veces complejo y representan una relación de constantes luchas y debates.

Ambos conceptos hacen parte de la cotidianidad física y digital, involucrando la opinión y la voluntad misma de las personas en tanto es normal hablar sobre cámaras, datos, rastreo, huellas, seguimiento, y demás terminología relacionada. Dentro de este constante acercamiento, diálogo y debate se cuestiona la situación actual respecto a estos temas dentro de un contexto de las TIC's, por lo que puede sugerirse la existencia de una agenda pública interesada en los flujos de información dentro de la Web que con insistencia exigen al Estado y al mercado hacer un uso responsable de los datos que poseen y de las herramientas que utilizan para tener un acceso extendido a estos, que posibilitan innovadoras pero cuestionables funcionalidades para generar información con fines poco (o no) conocidos por la ciudadanía que usa Internet.

Al conocer esta resistencia civil se puede reconocer un desaliento de una parte de la sociedad que desea mejorar algo respecto que el Estado o el mercado no está haciendo o está haciendo de maneras reconocidas como malas prácticas. En este contexto se puede afirmar que la vigilancia y la privacidad de la ciudadanía son

aspectos de interés para la sociedad y que existen dentro de la concepción de ciudadanía, conformando derechos humanos básicos dentro de un sistema político de carácter democrático.

Los resultados de esta investigación aportarían a los esfuerzos ya alcanzados por aquellos investigadores que se han interesado en el tema en Latinoamérica desde diferentes áreas del conocimiento como sociología, psicología, ingeniería, etc. Desde los estudios de los medios masivos de comunicación los enfoques han sido variados, sin embargo, la cobertura de estos temas (ver en el apartado 1.2.1.1. Análisis de medios acerca de privacidad y vigilancia) no ha sido abordada en Latinoamérica, por lo que se supondría un aporte para agregar contexto a un tema que lo requiere y exige mayor profundización.

Al realizar un esfuerzo por entregar información de contexto para temas tan amplios como la vigilancia y la privacidad ciudadana, se está haciendo un trabajo que entrega otra perspectiva alrededor de la construcción de este fenómeno en la actualidad. Los medios masivos de comunicación ponen en la agenda pública realidades desde una posición determinada por muchos factores; no es correcto afirmar que lo que muestran diariamente es neutral puesto que cada decisión editorial está determinada por intereses e interesados alrededor de los hechos a los cuales se les presta determinada atención y enfoque. Por tanto, en una medida práctica no se pretende dar una solución directa al problema, mas si problematizar la posición de la prensa escrita digital respecto estos temas.

En esta medida existe una relación entre vigilancia, privacidad de la ciudadanía, y la agenda de los medios de comunicación masiva sobre estas temáticas en un contexto político-económico específico que puede contextualizar y robustecer las condiciones desde las cuales posicionan de una u otra manera dicha agenda; ya decía Fowler (1991), citado por Branum & Charteris-Black (2015), los contenidos

de la prensa disponen en la esfera pública "creencias, valores e ideologías construidas lingüísticamente".

Es acá donde se encuentra un espacio particular en el cual se puede profundizar sobre el fenómeno de la vigilancia y la privacidad de la ciudadanía haciendo uso de metodologías propias del área de la comunicación con el fin de develar los significados y el tratamiento que se hace a la información obtenida de los hechos o noticias tomadas como muestra para el estudio. Se realiza un estudio en el que se aplica teoría de la comunicación para profundizar en dos fenómenos, sin embargo, no se pretende realizar un desarrollo teórico adicional al área.

Al aplicar este estudio al tratamiento periodístico de dos temáticas internacionalmente reconocidas y tratadas en un país como Colombia representa una importancia inmediata de alto interés para la academia, en tanto la situación actual del país con un proceso de paz firmado y con recurrentes incidencias en las cuales la vigilancia y la privacidad de la ciudadanía se ponen en discusión (Fundación Karisma, 2016), se puede justificar que un estudio desde el análisis de los medios de comunicación masivos como ejemplos de unas percepciones y realidades resulta de más esclarecedor sobre las causas por las cuales se muestra cierta información con un tratamiento específico y que enmarca una gran realidad (M. McCombs & Ghanem, 2001), por llamar de alguna manera realidad a todo lo que sucede alrededor de los fenómenos mencionados.

#### 1.2.1.1. Análisis de medios acerca de privacidad de la ciudadanía y de vigilancia estatal

En este contexto sobresale la duda acerca de la posición de los medios de comunicación respecto a los temas de vigilancia y privacidad en Colombia e identificar si existe una agenda. Se ha realizado una revisión sobre literatura que haya hecho acercamientos desde la teoría de los medios de comunicación a los

temas de vigilancia y privacidad, y se ha encontrado que desde el análisis de contenido se ha abordado el tema de la privacidad (Fornaciari, 2014; Roznowski, 2003) y desde el análisis de discurso se han abordado tanto la privacidad (John & Peters, 2017; Kumpu, 2012) como la vigilancia (Barnard-Wills, 2011). También se destacan los abordajes desde el análisis crítico de discurso a la vigilancia (Branum & Charteris-Black, 2015; Lischka, 2017). Dentro de esta misma literatura sobresalen los tratamientos a la privacidad (Fornaciari, 2014) y a la vigilancia (Barnard-Wills, 2011; Branum & Charteris-Black, 2015) desde las teorías de *Framing* y *Agenda setting*, así como aquellas que son tratadas desde la *agenda setting* únicamente (Lischka, 2017; Roznowski, 2003).

Si bien los estudios mencionados anteriormente han salido directamente de la academia, estudios a destacar en esta área para Latinoamérica son resultados de ONGs como Fundación Karisma y Dejusticia de Colombia, Derechos Digitales de Chile, Privacy International de Gran Bretaña y Electronic Frontier Foundation de Estados Unidos quienes han desarrollo en los últimos dos años reportes en los que se han abordado directamente las problemáticas de vigilancia y privacidad en Colombia, territorio objeto de este trabajo y que sin este valioso aporte sería aún más complejo el acceso a información de estas características (Ver Anexo I, para ver listado de informes).

### 1.2.2. Privacidad de la ciudadanía y vigilancia estatal en el mundo

Desde el ataque del 9/11 en New York, la sociedad norteamericana y, consecuentemente el mundo entero, se vio inmerso en una nueva forma de ver y asumir la vigilancia como método de seguridad (Sosa Troya, 2015). Con el desarrollo acelerado de las tecnologías en Internet y el cambio de paradigma de los consumidores a productores de información, el flujo de información personal aumentó, siendo coleccionada y organizada por empresas de telecomunicaciones y por empresas que ofrecen servicios en la web (como correo electrónico, mensajería

instantánea, compartimiento de información en diversos formatos, etc.) (Parliament of United Kingdom, 2009). La convergencia de estos dos hechos, permitió a los gobiernos crear robustos discursos políticos basados en la seguridad, visión desde la cual empezaron a legitimar la necesidad de vigilar a los ciudadanos; un ejemplo claro de este caso fue revelado por Edward Snowden (Snowden, Poitras, & Greenwald, 2013) sobre los sistemas de vigilancia estatal por parte del estado norteamericano (PRISMA) y del estado británico (Tempora) compuestos por tecnologías especializadas que permiten monitorear, interceptar, coleccionar, categorizar y preservar datos e información de carácter personal de todas las personas que navegan por Internet, hablan por telefonía celular, se movilizan con un dispositivo GPS, etc.

Esta situación de vigilancia estatal vulnera una serie de derechos humanos como la "libertad de opinión y expresión, libertad de agrupación y asociación, derecho a la vida en familia y la salud" (Organización de las Naciones Unidas, 2014) lo que pone en duda la licitud y la legalidad de los sistemas de vigilancia que están siendo implementados y ejecutados en diferentes partes del mundo. En este mismo orden, al hablar de vigilancia estatal no es posible dejar a un lado la privacidad de quien es objeto del acto de vigilancia; en este contexto, la privacidad es un derecho humano fundamental que preserva la libertad y la autonomía, siendo esencial en una democracia (Kerr & Barrigar, 2012).

Si bien la ciudadanía hace uso de las TIC's, la comprensión sobre cómo funcionan resulta muchas veces de baja importancia o en definitiva irrelevante. Andrejevic (2014) justifica en esta medida una brecha entre las capacidades técnicas y el *know how* de las instituciones públicas y privadas, en comparación al de la ciudadanía en general sobre temas relacionados a las TIC's. Llama la atención esta diferencia que conlleva a una idea generalizada sobre una neutralidad de las TIC's en la

humanidad poniendo en riesgo los posibles desarrollos que traspasen límites de otros derechos humanos.

América Latina no ha estado exenta a esta situación, ya que se ha caracterizado por ser una ubicación donde la violencia ha sido una marca en el transcurso de su historia social, y la vigilancia estatal una historia con una existencia también de largo alcance (Arteaga Botello, 2015).

### 1.3. Pregunta general

¿Cuál es la agenda de la prensa escrita digital respecto a los temas de la privacidad de la ciudadanía y la vigilancia estatal en Colombia durante el periodo 2015-2016?

#### 1.3.1. Preguntas específicas

**a.** ¿Cuál es el contexto social político de Colombia durante el periodo 2015-2016?

**b.** ¿Cuál es la cobertura sobre los temas de vigilancia estatal y privacidad de la ciudadanía en la prensa escrita digital en Colombia, específicamente sobre los sistemas de vigilancia estatal y el caso de *Hacking Team*?

**c.** ¿Cuál es la construcción de realidad que entrega la prensa escrita digital en Colombia sobre vigilancia estatal y privacidad de la ciudadanía, específicamente sobre los sistemas de vigilancia estatal y el caso de *Hacking Team*?

### 1.4. Objetivo general de investigación

Describir y analizar la agenda de la prensa escrita digital respecto a los temas de la privacidad de la ciudadanía y la vigilancia estatal en Colombia durante el periodo 2015-2016.

### 1.4.1. Objetivos específicos de investigación

**a.** Describir el contexto social político de Colombia durante el periodo 2015-2016

**b.** Identificar la cobertura sobre los temas de vigilancia estatal y privacidad de la ciudadanía en la prensa escrita digital en Colombia, específicamente sobre los sistemas de vigilancia estatal y el caso de *Hacking Team*.

**c.** Describir la construcción de realidad que entrega la prensa escrita digital en Colombia sobre vigilancia estatal y privacidad de la ciudadanía, específicamente sobre los sistemas de vigilancia estatal y el caso de *Hacking Team*.

# CAPÍTULO II. MARCO TEÓRICO

Con el fin de acercarse al objetivo general de este trabajo, es menester separar las categorías conceptuales que se asumen para su desarrollo, en tanto unas categorías son propias de los estudios en comunicación social y otras pertenecen a áreas interdisciplinares, en este sentido: en primera instancia se atienden aquellas categorías de primera atención para este trabajo (Vigilancia y privacidad de la ciudadanía) y en segunda instancia las categorías que apoyarán el análisis desde el propio campo de la comunicación (*Agenda setting* y *Framing*).

Sin embargo, a modo contextual, se optó primero por hacer evidencia del contexto socio-político de Colombia, y la situación de la privacidad de la ciudadanía y la vigilancia estatal en este país, para posteriormente pasar a la conceptualización misma del presente trabajo y que se plantea en el párrafo anterior.

## 2.1. Contexto socio-político de Colombia durante los años 2015-2016

La violencia sigue siendo uno de los mayores problemas de la sociedad colombiana, la presencia de grupos armados ilegales permite hablar de un conflicto armado interno de más de 50 años de antigüedad y que no ha dado tregua ni al Gobierno ni a la ciudadanía, siendo ésta última la más afectada. Dichos grupos armados pueden ser identificados principalmente en tres bandos: las guerrillas de izquierda, los paramilitares de derecha, y las fuerzas armadas de Estado; estos bandos han cometido abusos a la ciudadanía durante su existencia, incluyendo crímenes de lesa humanidad, y en el periodo estudiado no se han quedado atrás (Human Rights Watch, 2017). El efecto de este conflicto ha dejado como resultado cerca de 45.000 desaparecidos, 27.000 personas secuestradas, 220.000 personas asesinadas y 6´900.000 personas desplazadas, números que representan la importancia de la violencia en la esfera pública de Colombia (Grupo de Memoria Histórica, 2013).

Durante 2015 y 2016 la realidad político social de Colombia estuvo marcada fuertemente por el proceso de paz con las Fuerzas Armadas Revolucionarias de Colombia - Ejército del pueblo (FARC-EP) realizado en la Habana, Cuba desde el 2012, llegando a un acuerdo para ser refrendado a través de un plebiscito realizado el 2 de octubre de 2016. En este plebiscito la mayoría[1] votó por la no aprobación de estos acuerdos, lo que llevó a una renegociación de lo acordado para finalmente firmar y aprobar un nuevo acuerdo el 24 de noviembre de 2016. El resultado del plebiscito dejó en el ambiente una sensación de división entre los ciudadanos respecto tanto con los acuerdos de paz con las FARC como con las perspectivas políticas asumidas en estos (El Tiempo, 2017); adicionalmente, luego de la no aprobación de los acuerdos, el presidente Juan Manuel Santos fue condecorado con el Nobel de Paz, entendido como símbolo del apoyo internacional al proceso de paz.

Las FARC-EP no fueron y no han sido el único tema en cuanto a violencia contra del Estado se refiere en Colombia, también es válido mencionar la presencia, sin tanta cobertura como si lo tenían las FARC-EP, del Ejército de Liberación Nacional (ELN) con quienes se habían empezado a fines del 2014 unos diálogos de paz exploratorios que a fines del 2016 seguían en esa fase en tanto los representantes de dicha guerrilla estaban a la espera de la conclusión del proceso de paz con las FARC-EP. A pesar de la consecución de los diálogos de paz, la guerra en campo siguió durante 2015 (FARC y ELN) y 2016 (sólo el ELN), mostrando sin embargo una disminución visible de víctimas gracias al cese al fuego anunciado por las FARC a principios del 2015.

Paralelo a las guerrillas de izquierda, los paramilitares siguen siendo parte de una representación armada con tintes políticos de derecha, y con una cobertura no menor que no deja de llamar la atención porque pasaron por un proceso de desmovilización entre 2003 y 2006, pero que presentó sus fallas (Human Rights

[1] El resultado del plebiscito fue del Sí con un 49,79% y del No con un 50,21%, respectivamente, siendo 0,42% la diferencia.

Watch, 2017). Durante 2015 y 2016, los acuerdos de justicia y paz con los paramilitares se estaba ejecutando lentamente, pero con avances en investigación que llevaron a revelaciones sobre presuntos nexos de miembros y ex miembros del Gobierno con paramilitares.

El narcotráfico también es una realidad definitiva para la Colombia de los últimos 30 años, y sigue siendo parte de las acciones ilegales con mayor cobertura en el país y que tiene un efecto internacional. La llamada lucha contra las drogas se centra principalmente en dos ámbitos: la producción y la distribución, sin dejar a un lado los efectos secundarios de ambos procesos. Esta preocupación no se representó en números durante 2015 y 2016 y la cantidad de cultivos de coca aumentaron hasta llegar a un nivel similar al del 2001 (146.000 hectáreas) (Manetto, 2017). El narcotráfico sigue siendo uno de los principales patrocinadores del conflicto interno armado tanto para guerrillas y paramilitares, como el Estado.

Las Fuerzas Armadas por parte del Gobierno también han sido parte activa del conflicto interno armado. De los casos más nombrados es el de las ejecuciones extrajudiciales, comúnmente llamados 'falsos positivos', realizadas entre 2002 y 2008, en los que la fuerza pública ejecutaba civiles para hacerlos pasar como bajas en combate de guerrilleros. Durante el 2015 y 2016 las investigaciones siguieron su curso principalmente sobre los mandos inferiores y de generales que estuvieron prestando servicio durante el periodo cubierto de las investigaciones al respecto.

A razón de los diálogos y acuerdos de paz llevados hasta 2011, se promulgó la Ley 1448 titulada "Ley de Víctimas y Restitución de Tierras", cuyo propósito inicial es dar "atención, asistencia y reparación integral a las víctimas del conflicto armado interno" (República de Colombia, 2011). Esta ley con gran alcance y proyección para 2015 y 2016 venía avanzando, lentamente, teniendo efectos principalmente en las zonas rurales, las más afectadas por el conflicto armado.

Durante este periodo la realidad política y social del vecino país Venezuela estaba generando efectos directos e indirectos en Colombia. El cierre de la frontera por cerca de un año debilitó las relaciones diplomáticas generando la deportación de 2.000 colombianos y el regreso Colombia de 18.000 compatriotas que dejaron de sentirse con la suficiente estabilidad social y económica dentro de Venezuela (República de Colombia, 2017).

Dentro de los acuerdos de paz con las FARC-EP, existía un punto fundamental que era el ingreso a la política de sus integrantes interesados en ello. En este marco, muchas personas en desacuerdo en la forma en que esto se acordó han optado por tomar como ejemplo el momento de Venezuela como un posible resultado de lo que sería tener a las FARC-EP en puestos de poder político y gubernamental; si bien esto tiene muchos matices y verdades, el "castrochavismo" surge durante el 2015 y 2016 como un elemento con mucha fuerza de convencimiento y reforzado por cuatro razones principales: la debacle del modelo socialista cubano y venezolano, la influencia en el país de Álvaro Uribe[2] (principal contradictor de los acuerdos de paz con las FARC-EP), el miedo a las FARC-EP como líderes políticos (debido a su pasado violento), y las mismas equivocaciones del Gobierno en el establecimiento de los acuerdos y la comunicación a la ciudadanía (Revista Semana, 2017).

## 2.2. Privacidad de la ciudadanía y vigilancia estatal en Colombia

El Estado Colombiano tiene un historial particular para resaltar en este campo. Tanto legal como técnicamente ha realizado esfuerzos para la implementación de tecnologías de vigilancia con capacidades de recopilación de información desde los diferentes servicios de inteligencia: Departamento de Inteligencia de la Policía (**DIPOL**), de la antigua Dirección Central de Policía Judicial e Inteligencia (**DIJIN**),

[2] Presidente de Colombia 2002-2008, Senador de la República 2014-2018, y principal líder del Partido Político 'Centro Democrático'.

hoy conocida como Dirección de Investigación Criminal e Interpol, y del Departamento Administrativo de Seguridad (**DAS**).

Los primeros antecedentes que tuvieron reconocimiento a nivel nacional e internacional en el ámbito de vigilancia estatal en Colombia fueron las interceptaciones ilegales en 2009 por el DAS, conocidas como 'chuzadas'. Estas interceptaciones se ejecutaron a las conversaciones telefónicas de "magistrados de la Corte Suprema de Justicia, políticos de partidos de oposición, miembros de ONG, entidades internacionales de derechos humanos y periodistas" (Revista Semana, 2009); el caso, que no ha sido el primero en Colombia, demostró un bajo nivel de funcionalidad entre los diferentes servicios de inteligencia, poco control externo de otros organismos de Estado y ciudadano, y constantes preocupaciones sobre su legitimidad y eficiencia (Cepik & Ambros, 2014). Por este caso, y otros, el DAS fue liquidado en el 2011 y reemplazada por la Agencia Nacional de Inteligencia (**ANI**) la cual permitió y gestionó la Ley 1621 del 17 de abril de 2013, conocida como Ley de Inteligencia, que pretende ser el mandato que organiza la inteligencia y contrainteligencia ejecutada legalmente desde la ANI, evitando irregularidades antes evidenciadas. Sin embargo, aún se presentan vacíos que dan pie a violaciones desde las actividades que allí se ejecutan (Cortés Castillo, 2014).

Otro caso que evidenció prácticas de vigilancia estatal en Colombia fue la publicación del Decreto 1704 de 2012 que obliga a los proveedores de telecomunicaciones (UNE, Telefónica, Emcali, Telebucaramanga, Metrotel, Telmex, ETB y EPM) como a las redes de datos móviles (Claro, Tigo, Avantel y Movistar) a crear *backdoors,* herramientas que facilitan la monitorización de las comunicaciones por parte del Estado (Rodríguez, 2012). Esto permitía al Estado, con el uso de diferentes herramientas tecnológicas, acceder a la información que los proveedores recopilaban de los clientes que hacen uso de sus redes. Además de esto, la telefonía móvil en Colombia no está encriptada (Hosein, 2014) lo cual

representa una serie de graves problemas de seguridad para los usuarios mismos frente a la presencia de *hackers* con intenciones contrarias al respeto por la información y el espacio digital del otro.

En el mes de agosto de 2015, Privacy International publicó dos reportes sobre vigilancia en Colombia (Privacy International, 2015a; Privacy International, 2015b) que permiten verificar y realizar un mapeo de las empresas privadas, organismos del Estado Colombiano y tecnologías involucradas en lo que ha resultado ser todo una apuesta por establecer un Sistema de vigilancia potente y robusto para la monitorización, interceptación, colección, categorización y preservación de información personal de la ciudadanía Colombiana registrada desde diferentes dispositivos (celular, Internet, GPS, etc.). De manera resumida, los reportes muestran una estructura donde el estado Colombiano, desde diferentes organismos propios (DIJIN, DAS DIPOL) ha tenido tres sistemas de vigilancia (Esperanza, PUMA y SIGD), con fines similares pero que difieren en controles por parte del Estado (Fiscalía General de la Nación o desconocido), en el tipo de vigilancia (selectiva y masiva), y en las tecnologías de interceptación táctica.

A mediados de 2015, igualmente se develó la existencia de una relación contractual entre el Estado Colombiano y las empresas Robotec Corporation y NICE Systems, representantes de la empresa italiana de vigilancia estatal Hacking Team (Durán Núnez, 2015; Pérez de Acha, 2016), cuya especialidad es un *software* llamado *Remote Control System GALILEO* (RCS) que permite interceptar computadores, llamadas por skype, correos electrónicos, mensajes instantáneos, contraseñas, etc., es decir, todo lo que tiene que ver con la vida privada de las personas, además de tener el control de las funcionalidades de *hardware* del dispositivo hackeado (cámara, micrófono, GPS, etc.). RCS fue suscrito en el periodo de 2013 a 2016 (con Robotec Corporation) y negociado para su renovación hasta 2018 (con NICE Systems) por la Policía Nacional de Colombia, y ha tenido gran acogida en toda la

región latinoamericana y a nivel internacional (Pérez de Acha, 2016); es en esta revelación que se identifica que PUMA es en la práctica RCS.

Debido al alcance de interceptación de RCS, se logran identificar violaciones a la privacidad, a la libertad de expresión y al debido proceso (Pérez de Acha, 2016), desmarcándolo de toda interpretación legislativa y judicial y manteniendo, más abierta que nunca antes, la discusión de cómo la ley puede estar a la par de las implicaciones de los avances tecnológicos.

La mera existencia de estos reportes justifica una importancia del tema de la vigilancia estatal y la privacidad de la ciudadanía para disponer en la esfera pública del país y, por tanto, demanda una profundización multidisciplinar que logre describir y, si es posible, explicar una realidad aún un poco abstracta para las personas del común, pero que eventualmente puede generar problemas en la forma en que estamos en sociedad.

### 2.3. Vigilancia social e institucional en el entorno de redes digitales

Acercarse a conceptos de vigilancia y privacidad de la ciudadanía puede variar según la aproximación entendiendo que son categorías trabajadas multidisciplinariamente. De todas maneras, Elmer (2012) indica como la base de los estudios de vigilancia la construcción teórica realizada por Jeremy Bertham, Michel Foucault y Gilles Deleuze quienes en diferentes momentos históricos han buscado explicaciones teóricas involucradas en el funcionamiento de sociedad occidental desde tres conceptos fundamentales, respectivamente: panóptico, disciplina y control; estas visiones se centran principalmente en una vigilancia situada en las rutinas institucionales y las relaciones dentro de la sociedad (Lyon, Haggerty, & Ball, 2012) y que han estado definidas para cada momento histórico de la sociedad occidental como elemento crucial de su funcionamiento.

Estas concepciones de vigilancia han estado ajustadas a las mismas formas en que esta se ha implementado y ejecutado a través de la historia de la humanidad. Marx (2016) diferencia unas formas tradicionales de vigilancia, propias de las sociedades pre-industriales, de unas nuevas formas de vigilancia propias de las sociedades industriales que desde su interior han desarrollado evolucionadas herramientas de continua especialización que han permitido un mayor alcance y trascendencia en la sociedad. Esta nueva vigilancia es definida como: "*scrutiny of individuals, groups, and contexts through the use of technical means to extract or create information*" (Marx, 2016). Este acercamiento al concepto deja por fuera toda vigilancia dada en la vida cotidiana a partir de medios no técnicos/tecnológicos a propósito del mismo objetivo del presente trabajo de investigación.

La nueva vigilancia cuenta con algunas características particulares que valen la pena mencionar con la finalidad de puntualizar su existencia en la sociedad actual, a saber:

- Deja de ser necesariamente particular o direccionada a una persona sospechosa, pasa a poner como objetivo contextos (lugares, espacios, períodos de tiempo, redes y sistemas).

- La vigilancia se puede dar desde cualquier punto geográfico y a cualquier nivel, caso que antes por posibilidades técnicas era necesario hacerlo de cerca únicamente; de ahí que se diga que la vigilancia se haya vuelto más lejana (en cuanto espacio físico) y más cercana (en cuanto a información recolectada) que antes.

- En toda estructura de vigilancia habrá un agente, un sujeto y una audiencia (opcional, en los casos que la información se hace pública). La diferenciación entre el agente y el sujeto eran fácilmente identificables en la vigilancia tradicional, sin embargo, en la nueva vigilancia cualquier persona tiene la

posibilidad de ser agente, sujeto e inclusive agente-sujeto en los casos de auto vigilancia (*self-surveillance*).

- Las nuevas formas de vigilancia en muchos casos son imperceptibles o, de facto, invisibles. Por tanto, lo que un sujeto sabe acerca de lo que un agente sabe de él/ella, es más borroso.

- Los datos o información recolectada en muchos casos, al ser automáticamente recolectada, no alcanza a tener una calidad de contenido contextualizada, en cambio, se relaciona con base a funciones matemáticas y algorítmicas que no cuentan con la misma capacidad de contar algún suceso que representa como si lo puede contar el sujeto que lo protagonizó.

Para encontrar la sistematización de estas características se puede consultar el Anexo II, donde se replica un paralelo realizado por Marx (2016) entre la vigilancia tradicional y la nueva vigilancia.

Esta vigilancia puede tener diferentes propósitos de protección, administrativos, de documentación o estratégicos, pero algunos de mayor atención como manipulación inapropiada de información, control social o espionaje ilegal, a todo nivel de socialización ya sea entre amigos, en el trabajo, en la familia o desde el gobierno (Marx, 2007) . Fuchs (2011a) argumenta que esta vigilancia se puede caracterizar por su aspecto de negatividad en el poder de las estructuras sociales, la sociedad contemporánea, y las sociedades heterónomas, en definitiva, usa su definición para indicar y denunciar la dominación en la sociedad.

En la actualidad se puede hablar de una vigilancia de mayor alcance denominada masiva (Fuchs, 2011) que es definida como el "hecho de monitorizar el comportamiento de otro ya sea en tiempo real usando cámaras, dispositivos de

audio o *keylogger*[3], o en determinado momento por minería de datos de las transacciones en Internet" (Wall, 2007).

## 2.4. Privacidad de información e integridad contextual

Al hablar de vigilancia es necesario remitirnos al concepto de privacidad como elemento constitutivo para su comprensión y tratamiento teórico y práctico. De hecho, ambos conceptos en la práctica bien pueden ser trabajados paralelamente para alcanzar diferentes objetivos ya que, si bien la vigilancia puede invadir la privacidad, puede también ser un medio de su protección; viceversa, la privacidad puede proteger la vigilancia pero también puede anularla (Marx, 2016). Estas interrelaciones entre la privacidad y la vigilancia son fundamentales al momento de tratarlas conjuntamente como categorías de análisis.

La privacidad, tal como se afirmaba con la vigilancia, es un área multidisciplinaria que requiere de una acotación para su aplicación a un contexto específico, entendiendo que es un producto de normas, actividades y protecciones legales que varían de país en país. Es común relacionar el concepto de privacidad a discreción, soledad, seguridad, confidencialidad, entre otros y que al momento de describirlo se confunda con estos u otros conceptos (Tavani, 2008).

Sin embargo, la privacidad es primero un derecho humano (Organización de las Naciones Unidas, 2015) , fundamental para las sociedades democráticas modernas, a pesar de que no es conocido cuál ha sido su evolución a través de la historia reciente con el advenimiento y posicionamiento de las TIC's (Fornaciari, 2014). La propuesta de Solove (2010) apunta a una construcción conceptual de la privacidad como una pluralidad de varias cosas relacionadas entre sí, es una construcción social establecida a través de normas y leyes acerca de algo que las personas

[3] Es un software que permite el registro de los tipeos del teclado en tiempo real de un equipo seleccionado.

desean mas no de algo que ellas esperan, es decir, históricamente la privacidad se ha formado como un deseo y no como una expectativa.

Para comprender esto, Solove (2010) ha desarrollo un marco de problemas que atañen a la privacidad y que son los siguientes: colección de información, procesamiento de información, diseminación de información e invasión. Sin embargo, la concepción de información acá merece ser profundizada, y Tavani (2008) desarrolla cuatro tipos de privacidad que conciernen a su comprensión:

- **Privacidad física:** Libertad de cualquier intrusión física y, por tanto, a la posibilidad de estar solo.
- **Privacidad decisional:** Libertad a la interferencia de algo o alguien en la toma decisiones personales e íntimas.
- **Privacidad psicológica:** Libertad de cualquier interferencia psicológica, siendo esencial para la protección de la integridad de personalidad del sujeto.
- **Privacidad de información:** Libertad de cualquier interferencia y por tanto, la existencia de restricciones de acceso a hechos acerca de algún sujeto cualquiera, entendiendo a información a cualquier registro de datos sobre las actividades diarias, estilos de vida, finanzas, historial médico, o logros académicos.

Entendiendo el contexto determinado en los antecedentes y objetivos del presente trabajo, la privacidad de información es la categoría y enfoque que se tendrá en cuenta para el análisis que posteriormente se documenta.

La privacidad de información se entiende de diferentes maneras según el contexto en el que se esté evaluando, entendiendo que la sensibilidad, entiéndase confidencialidad, de la información es un factor clave al momento de evaluar la

cualidad de privacidad que se considere oportuna nominar (Noain Sánchez, 2015). Dicha sensibilidad puede variar dependiendo del momento y del lugar (tiempo y espacio), por lo que una conceptualización más holística de privacidad informacional con una integridad contextual resulta más oportuna y flexible para su aplicación en el presente trabajo que cuenta con sus propias delimitaciones contextuales; adicionalmente, esta integridad contextual ha sido diseñada en un marco de los nuevos medios de comunicación que han puesto en una línea más difícil de determinar lo privado, o aquello que merece una cualidad de sensibilidad determinada (Nissenbaum, 2010 citada por Fornaciari, 2014).

Concentrando estos acercamientos teóricos a la realidad de las tecnologías de información y comunicación de hoy desde y en las cuales se participa en la cotidianidad, el derecho a la privacidad no es más que el derecho al control sobre el cosechamiento, categorización, almacenamiento y uso de datos que transitan en las diferentes redes donde circulan análoga y digitalmente.

Como el objetivo del presente trabajo proyecta, se pretenden abordar los temas de vigilancia y privacidad de la ciudadanía desde su tratamiento en los medios de comunicación, puntualmente en la prensa escrita digital, optando como bases teóricas los conceptos de *Agenda setting* y *Framing*, los cuales permitirán definir la existencia de una agenda y, si existe, describirla. Si bien ambos conceptos han sido ampliamente tratados aún se les tiende a asignar características similares y, por ende, a no diferenciarlos propiamente. A continuación se atenderán ambos conceptos por separado y se concluye con una propuesta de abordaje conjunta.

## 2.5. *Framing* y *Agenda setting*: diferencia de enfoque

El *framing* o teoría del encuadre puede definirse desde la construcción de realidad que se hace tanto desde el emisor como del receptor. Si bien a partir de esto se puede construir una teoría compleja del *framing* en el que intervienen todos los

encuadres construidos en un momento determinado desde cualquier formato de comunicación, análogo o digital, para el presente trabajo interesa el *framing* de los medios de comunicación como construcción de la realidad, el cual es definido como "el proceso por medio del cual las personas desarrollan una conceptualización particular de un tema (*issue*) o reorientan su pensamiento acerca de dicho tema" (Chong & Druckman, 2007). Desde una descripción comparativa, el proceso de *framing* se asemeja al proceso de fotografía, en tanto la persona encargada de tomar la imagen tiene que, por obligación, dejar a un lado lo que queda fuera del lente y respecto a lo que está tomando es porque tiene unas características primordiales a tener en cuenta para mostrar a un público objetivo.

Por esta necesidad de enmarcar los hechos y las realidades, es que la teoría de *framing* se fundamenta en la premisa de que un tema puede ser visto, conceptualizado y construido desde una variedad de perspectivas, con múltiples implicaciones de valor y consideración (Chong & Druckman, 2007). Determinados hechos o realidades enmarcadas se les denomina *frames,* o 'fotografías' retomando la anterior analogía, que son definidos como "una idea central organizadora o una línea de relato que proporciona significado a un conjunto de acontecimientos, tejiendo una conexión entre ellos" (Gamson & Modigliani, 1987 citado por Chong & Druckman, 2007). De tal manera el *frame* simplifica la comprensión de una realidad o hecho, concretando allí la información más relevante y que tiene alguna conexión con su contexto (Ardèvol-Abreu, 2015); vale la pena apuntar que esta simplificación se da en un orden técnico, es decir, no es posible hablar de toda una realidad como tal, pero también se da por un interés particular basado en unos valores o consideraciones propios del autor y/o su afiliación (institucional, política, personal, etc.). Así se puede afirmar que un *frame* se construye con varios esquemas*:* el del periodista (productor), el del receptor, en los subtextos y en la cultura (desde la cual se generan y construyen) (Oller Alonso, 2014).

Por tanto el *frame* en los medios de comunicación cuenta con cuatro dimensiones: los subtemas de las noticias, los mecanismos que encuadran (tamaño y ubicación), los atributos cognitivos y los atributos afectivos Ghanem, 1997 citado por Oller Alonso, 2014; los atributos cognitivos permiten identificar el carácter significativo de los temas, mientras que los afectivos se centran en el tono y estructura narrativa de la historia (Oller Alonso, 2014). Es a partir de estas dimensiones que se pueden hallar los puntos más importantes de un encuadre elegido, porque son estos mismos los que en algún momento definieron su enfoque.

La *Agenda setting* entra en escena en un momento más amplio del medio de comunicación, pues ya no determina cómo abordar determinada realidad o hecho, sino cuál sería la posición completa del medio para abordar diferentes temáticas de diferente orden social, político y económico de una manera coherente a unos intereses de primer orden para hacer visible a las audiencias dichas realidades/hechos enmarcadas. El poner en la agenda alguna realidad por encima de otras, es un proceso denominado tematización (*thematization*), que al final termina siendo relevante cuando se sitúa tanto en la agenda del medio como en la agenda de la opinión pública (Oller Alonso, 2014).

La *agenda setting* se refiere así a "la idea de que hay una fuerte correlación entre el énfasis que el medio de comunicación pone a ciertos temas (por ejemplo, basado en el lugar que aparece dentro de la publicación o la cobertura), y la importancia atribuida a dichos temas por las audiencias" (McCombs & Shaw, 1972 citado por Scheufele & Tewksbury, 2007). En este sentido, se le da una importancia no sólo a los temas que hacen parte de una agenda, sino al tratamiento y orden que se le da a los mismos a partir de los diferentes aspectos que los describen; el alcance de la *agenda setting* como metodología es identificar los temas que los medios están predominando para que su audiencia objetivo tenga en cuenta en la esfera pública.

No habría así una sola agenda, sino tres: la agenda de los medios, la agenda pública y la agenda política (Oller Alonso, 2014).

El problema de estos dos conceptos radica en su diferenciación al momento de ser estudiados, y para ello Scheufele y Tewksbury (2007) ofrecen un análisis comparativo en el ciclo de vida de las noticias en tres fases: producción, procesamiento y recepción. Durante la fase de producción, al estar centrada en la construcción de mensajes, parece ser el enfoque de *framing* que permite con mayor precisión responder a la pregunta sobre cómo la sociedad construye los discursos acerca de un tema desde etiquetas predominantes, sin embargo, la *agenda setting* permite leer los factores externos que influencian los contenidos de las noticias.

Durante la fase de procesamiento, tanto la *agenda setting* como el *framing* parecieran operar de la misma manera, a pesar de que la atención que se le presta a los mensajes es pertinente estudiarla desde una teoría de *framing*, la exposición pública misma de una temática es suficiente para acercarse desde una teoría de *agenda setting*. Por último, en la fase de recepción, o de los efectos, en un primer nivel la *agenda setting* llama a pensar sobre determinados temas, y el *framing* llama a cómo pensar sobre dichos temas.

De esta manera, Scheufele y Tewksbury (2007) concluyen que la diferencia entre *agenda setting* y *framing* radica al nivel de los efectos de accesibilidad y aplicabilidad, respectivamente; la accesibilidad está basada en modelos de procesamiento de información basados en la memoria, y la aplicabilidad se refiere al resultado que sugiere la conexión de dos o más conceptos en un mensaje expuesto a la audiencia, y que ésta la acepte. De esta manera se puede afirmar que en el proceso de comunicación de los medios hacia las audiencias, la inclusión complementaria de *agenda setting* y *framing* es una necesidad, en tanto la primera permite contextualizar y la segunda profundizar la selección de los temas y los mensajes relacionados.

# CAPÍTULO III. DISEÑO METODOLÓGICO DE LA INVESTIGACIÓN

## 3.1. Enfoque de la investigación

Se realizó una investigación cualitativa definida ampliamente por Taylor, Bogdan y DeVault (2016) como aquella que produce información descriptiva desde las palabras habladas o escritas por las personas y desde comportamientos observables, siendo un camino de aproximación al entendimiento del mundo empírico.

Entendiendo que es un enfoque variado y de múltiples perspectivas de investigación según Patton (2002) citado por Vasilachis de Gialdino (2006), también puede ser definido como:

> *"un proceso interpretativo de indagación basado en distintas tradiciones metodológicas –la biografía, la fenomenología, la teoría fundamentada en los datos, la etnografía y el estudio de casos– que examina un problema humano o social. Quien investiga construye una imagen compleja y holística, analiza palabras, presenta detalladas perspectivas de los informantes y conduce el estudio en una situación natural"* (Creswell, 1998citado por Vasilachis de Gialdino, 2006).

Desde los estudios de la comunicación Jensen (2012) apunta a una conceptualización de la investigación cualitativa desde tres categorías comunes en varios estudios de referencia al respecto, que son: significado, contextos naturales y sujeto interpretativo. El significado es el factor denominador a toda investigación cualitativa, y toda persona y artefacto cultural es vehiculizador de este, siendo los medios de comunicación un ejemplo estrella como productor y distribuidor de significado. Los contextos naturales remite a la cuestión que enfrenta todo estudio cualitativo sobre la realidad a estudiar desde preguntas tanto epistemológicas

como éticas al momento de intervenir y que esto permita su correcta interpretación. Por último, el sujeto interpretativo se refiere directamente al investigador y su inevitable análisis e interpretación particular, que a pesar de estar en un marco epistemológico, teórico y metodológico debe partir de su experiencia en el área estudiada y por ende de sus palabras y análisis.

Como enfoque auxiliar al presente estudio, se utilizarán técnicas cuantitativas que enriquecerán el análisis, por tanto se argumenta que se pretende en definitiva una investigación de carácter cualitativo con rasgos cuantitativos.

### 3.2. Método de investigación

Teniendo en cuenta que el método de investigación obedece al tipo de información que se recogerá, analizará e interpretará, la etnometodología se constituye para el presente trabajo la guía para acceder a la información a través de un proceso de interpretación propio del análisis de contenido y análisis de discurso. Con base en el interaccionismo simbólico, la etnometodología se encarga de "estudiar los fenómenos sociales incorporados a nuestros discursos y nuestras acciones a través del análisis de las actividades humanas" (Rodríguez Gómez, Gil Flores, & García Jiménez, 1996), teniendo en cuenta que esta investigación se centrará en el uso de palabras y frases en los contenidos y discursos seleccionados en el corpus.

### 3.3. Tipo de investigación

Si bien los estudios sobre vigilancia y privacidad de información son amplios en la actualidad, se define que el presente estudio se encuentra en un espacio de investigación de carácter descriptivo en tanto pretende disponer de las bases de entendimiento de un fenómeno sin interesar particularmente el porqué de su comportamiento, es decir, se obtiene información contextual acerca del tema seleccionado para generar algunas explicaciones posibles a esto (Adams, Khan, & Raeside, 2014); tal como asevera Gilgun (2015), las investigaciones basadas en

narraciones o discursos, como la presente, tienden a quedarse en ser descriptivas, estando disponibles para posteriores interpretaciones y teorizaciones. En este sentido, las descripciones están consideradas en un primer nivel de análisis pues provienen de fuentes tanto primarias como secundarias.

Se puede argumentar así que este no es un estudio de carácter exploratorio porque el objeto de estudio se encuentra en unas bases sólidas de alta producción en el ámbito académico que permiten ubicarlo en un estado científico que requiere de mayor descripción para asentarlo en conceptos y realidades más palpables. Al hacer uso de estrategias de investigación relacionadas a los estudios en comunicación, se propone agregar valor contextual a las áreas en cuestión para el presente estudio desde la prevalencia y significado que los medios de comunicación proponen desde su agenda.

### 3.4. Muestra/Corpus

Se propone como universo de estudio la agenda de los medios de comunicación masiva sobre vigilancia y privacidad de la ciudadanía en Colombia, estableciéndose como corpus la agenda de la prensa escrita digital de los dos periódicos de mayor consulta en Colombia, El Tiempo (http://www.eltiempo.com/) y El Espectador (http://www.elespectador.com), sobre los contenidos noticiosos y de opinión de ambos periódicos producidos entre 2015 y 2016, dentro de dichos contenidos noticiosos se tendrán en cuenta aquellos relacionados a los siguientes hechos sobre vigilancia y privacidad de la ciudadanía:

| **Temas del presente trabajo** |
|---|
| Sistemas de vigilancia masiva estatal en Colombia |
| Hacking Team |

La selección muestral de estas temáticas se da en función de la cantidad de noticias por abordar en el presente trabajo, tomando en cuenta aquellos casos de los

intentos del Estado por implementar tecnologías de vigilancia masiva sobre la ciudadanía y que, por ende, ponen en duda su privacidad. De esta manera, se puede puntualizar desde estos casos qué y cómo se están acercando los medios de comunicación a los temas de privacidad de la ciudadanía y vigilancia en Colombia durante el periodo seleccionado.

Realizando una búsqueda en ambos periódicos, bajo los años 2015-2016, de los temas seleccionados, se obtienen 83 artículos noticiosos y de opinión que mencionan alguna de las siguientes temáticas:

- Sistemas de vigilancia masiva
- Hacking Team
- Vigilancia estatal masiva
- Vigilancia masiva
- Privacy International
- Vigilancia electrónica
- Vigilancia digital
- Plataforma Única de Monitoreo y Análisis (PUMA)
- Sistema Integrado de Grabación Digital (SIGD)

Para mayor detalle de las noticias seleccionadas, consultar Anexo III.

## 3.5. Técnicas de investigación

### 3.5.1. Técnicas de recogida de información

Se describen las técnicas de recopilación de información que se utilizarán en el presente trabajo para análisis posterior según la técnica de análisis seleccionada:

| OBJETIVO ESPECÍFICO | TÉCNICA DE OBTENCIÓN DE INFORMACIÓN | TÉCNICA DE ANÁLISIS DE INFORMACIÓN |
|---|---|---|
| Describir el contexto social político de Colombia durante el periodo 2015-2016 | Recopilación bibliográfica | Descripción social política en el espacio y tiempo seleccionados en el presente trabajo |
| Identificar la cobertura sobre los temas de vigilancia estatal y privacidad de la ciudadanía en la prensa escrita digital en Colombia, específicamente sobre los sistemas de vigilancia estatal y el caso de *Hacking Team*. | Recopilación de notas periodísticas publicadas en los sitios web de los medios seleccionados sobre las temáticas seleccionadas. | Análisis de contenido |
| Describir la construcción de realidad que entrega la prensa escrita digital en Colombia sobre vigilancia estatal y privacidad de la ciudadanía, específicamente sobre los sistemas de vigilancia estatal y el caso de *Hacking Team*. | Recopilación de notas periodísticas publicadas en los sitios web de los medios seleccionados sobre las temáticas seleccionadas. | Análisis de discurso |

### 3.5.2. Técnicas de análisis de la información: análisis de contenido y análisis de discurso

Se realizó un análisis de contenido bajo un paradigma lingüístico/estructuralista y un análisis del discurso bajo un paradigma pragmático relacional; citando a Mariño (2009) "mientras que el primero suele partir, en su fórmula más cuantitativa, de la contabilidad de las presencias de los valores de cada variable, el segundo persigue la emergencia de un mensaje común a los diferentes momentos de una narración". Si bien esta perspectiva es la más concurrente en la literatura y la academia respecto a los análisis de contenido y discurso, es menester profundizar en sus concepciones para demostrar puntos de encuentro necesarios entre ambas metodologías.

El análisis de contenido a pesar que tiene un uso más cuantitativo de los textos, puede apuntar a un doble enfoque: cuantitativo, porque permite identificar la frecuencia de valores, y cualitativo, puesto que permite identificar la presencia o

ausencia de categorías, agregándoles una interpretación en función de los objetivos de la investigación que los destaca (Gómez Mendoza, 2000); vale la pena destacar que la identificación de presencias puede darse de manera directa o indirecta, dependiendo de si el contenido es manifiesto o latente, respectivamente.

Si bien se hizo uso de las frecuencias de las categorías desde un análisis de contenido cuantitativo, se hizo énfasis en una aproximación cualitativa, en tanto esta a su vez tiene un doble objetivo: fuerza al objeto de análisis a revelar su estructura en un acercamiento de-totalizante que instiga en la relación entre los aspectos individuales y la apariencia general, pero esto lo logra con la finalidad de alcanzar una mirada holística, sin perder un contexto social que enmarca cada frase (Mayring, 2014). Desde este enfoque se permiten identificar aquellas categorías relevantes para el análisis de discurso posterior.

Partiendo de que los discursos son el medio y el resultado de una modelación, producción y reproducción del mundo a través del lenguaje, el análisis de discurso es el estudio del lenguaje en uso, entendiendo los significados y acciones que le acompañan y que este sustenta (Gee & Handford, 2012). Con esta definición es válido afirmar que el análisis de discurso tiene la capacidad de acercarse a diferentes niveles lingüísticos y contextuales de este, en su variedad de formatos y medios, tanto como comunicación como acción.

Con estas técnicas de análisis de información se puede estar hablando de una misma técnica de recogida información que se basó en la recopilación de todas las noticias producidas en los periódicos, secciones y cobertura establecida, a partir de la cual se construyó una base de datos accesible que fue trabajada desde el programa gratuito *AntConc* (http://www.laurenceanthony.net/software/antconc/). Para la búsqueda y sistematización de las noticias, se usó la base de datos *ProQuest* llamada *International Newsstream,* en la cual se ejecutó la siguiente estrategia de búsqueda:

**pub.Exact**("El Tiempo" OR "El Espectador") AND **ft**("Sistemas de vigilancia masiva" OR "Sistema de vigilancia masiva" OR "Hacking team" OR "vigilancia estatal masiva" OR "Vigilancia masiva" OR "Privacy international" OR "Vigilancia electrónica" OR "Vigilancia digital" OR "Plataforma Única de Monitoreo y Análisis" OR "Sistema Integrado de Grabación Digital" OR "SIGD")

Adicional a estas técnicas de análisis de la información, se realizó una recopilación documental que posibilitó la descripción del contexto social político de Colombia en el período 2015-2016, considerándolo un proceso necesario para contextualizar en un lugar y tiempo particular el análisis que se buscó de las categorías de vigilancia estatal y privacidad de la ciudadanía.

## CAPÍTULO IV. VIGILANCIA ESTATAL EN UN PAÍS EN PROCESO DE PAZ

Se realizó un análisis del tratamiento que se le da en los medios a la vigilancia estatal y la privacidad de información en relación con el contexto colombiano, destacando la relevancia de la legislación, la acción del Gobierno, el respeto por los derechos humanos y la contextualización de estos factores en el avance de un proceso de paz, pensando a futuro en un país en posconflicto. Finalmente, se aborda una generalidad importante en cuanto a la relación entre vigilancia estatal y democracia.

### 4.1. Colombia implementando sistemas de vigilancia

Cuando se habla de Colombia dentro de las noticias, se encuentra un espacio preocupante en el que la implementación de tecnologías de vigilancia no está realizada de manera propositiva sino más bien conflictiva a la realidad del país. Se encuentra que la percepción de estar vigilado es alta, los alcances de las tecnologías van en aumento y sin restricciones, legalmente se generan más dudas que certezas, y la sociedad colombiana (u otro objetivo que tuviese) no cuenta con las herramientas legales suficientes para enfrentar esta situación.

En este sentido se identifican los siguientes recortes:

> *"Todos en Colombia estamos convencidos de que nos "chuzan", es decir, que interceptan nuestras comunicaciones"*[4].
>
> *"Las filtraciones de Hacking Team permitieron dimensionar que la capacidad de vigilancia en Colombia es mayor de lo que creíamos y ahora lo comprobamos con dos informes sobre tecnologías de vigilancia que publicó la ONG británica Privacy International"*[5].
>
> *"En un país con hechos como las chuzadas del DAS, Andrómeda, las supuestas compras que la Policía hizo a la empresa Hacking Team y los seguimientos a las periodistas Vicky Dávila y Claudia Morales, lo que estos expertos recomiendan es que un documento Conpes de seguridad*

[4] El Espectador. 25 de julio de 2015.
[5] El Espectador. 3 de septiembre de 2015.

*digital debería incluir una mención a estos hechos y medidas para limitar estas acciones de instituciones que, por otra parte, tienen una tarea legítima en el tema de ciberseguridad"*[6].

*"... en Colombia una persona no puede consultar si existen o han existido en el pasado acciones de inteligencia en su contra, ni pedir su corrección, ni hay un juez que controle la realización de ciertas actividades de inteligencia que inciden en sus derechos fundamentales"*[7].

*"La información filtrada evidencia problemas de orden político, jurídico y ético tanto para Colombia como para Hacking Team"*[8].

*"Colombia ha desarrollado un sistema de vigilancia de comunicaciones poco transparente y sin controles, ahora sabemos que también tienen capacidad de interceptación de comunicaciones a objetivos seleccionados que va más allá de PUMA"*[9].

Los alcances a los que ha llegado la tecnología en vigilancia en Colombia han sido aplicados por la fuerza pública del Estado. Se ha demostrado que esta fuerza pública ha participado en la adquisición y uso de tecnologías de vigilancia, sin embargo, también ha sido revelado que estas acciones han sido con base a dudosas o inexistentes bases legales, o con pocos controles administrativos. Por tanto, pone en cuestión la confianza en la fuerza pública del Estado, lo cual no es excepción en el entramado de esta en su función de proveer seguridad a la sociedad colombiana. Esto se identifica en los siguientes recortes:

*"La respuesta de la entidad fue un comunicado en el que indicó que "el propósito de esta compra fue potencializar la capacidad de detección de amenazas del terrorismo y la criminalidad organizada en el ciberespacio". En un país como éste, que la Fuerza Pública recurra a todas las herramientas posibles para combatir el crimen es lo mínimo que los ciudadanos esperan"*[10].

*"En la Policía, se supone -el general Palomino podría explicar mejor-, también hay controles internos. ¿Puede un país como Colombia confiar en el autocontrol de sus autoridades? ¿Es suficiente el autocontrol con programas como "Galileo", cuyos fabricantes aseguran que solo quienes tienen acceso a él (los investigadores judiciales) pueden rastrear su uso, dificultando establecer cuándo la herramienta fue usada?"*[11].

[6] El Espectador. 4 de febrero de 2016.
[7] El Espectador. 20 de mayo de 2015.
[8] El Espectador. 10 de julio de 2015.
[9] El Espectador. 3 de septiembre de 2015.
[10] El Espectador. 11 de julio de 2015.
[11] El Espectador. 18 de julio de 2015.

*"Colombia, como cualquier otro país, necesita herramientas para combatir la criminalidad. Pero el software de espionaje que escogió para hacerlo, el RCS de Hacking Team, ha sido duramente cuestionado desde antes de que Colombia lo adquiriera"*[12].

## 4.2. Leyes sobre vigilancia estatal y tratamiento de datos

Se encuentran menciones y tratamientos acerca de las leyes existentes en torno a los sistemas de vigilancia y a la privacidad de información en Colombia. Se encontró una ley, no mencionada en este trabajo, que es la Ley 1273 de 2009, en la cual "se preservan integralmente los sistemas que utilicen tecnologías de la información y las comunicaciones", que entiende como delito el mal uso de sistemas informáticos o desarrollo y circulación de software malicioso; con esta ley se pone a prueba es si la adquisición y uso de los sistemas de Hacking Team, al usar software malicioso para hacer interceptación, es enteramente lega. Se muestra en el siguiente recorte:

*"A raíz de la filtración de Hacking Team, la policía colombiana reconoce que tiene CNE desde 2013, sin mencionar el marco legal que soporta su uso, lo que sí sabemos es que tanto el acceso abusivo a sistemas informáticos, como el desarrollo y circulación de software malicioso son delitos (269E y 269F, Ley 1273/09)"*[13].

Respeto a la protección de datos, se dispone de la Ley 1581 de 2012 "Por la cual se dictan disposiciones generales para la protección de datos personales" y es la cual debe ser tenida en cuenta por parte de los prestadores de servicios de telecomunicaciones respecto a la información y datos que guardan y transitan a través de sus servidores y redes. Se menciona en recortes como el siguiente:

*"... es importante manifestarle que nuestras empresas afiliadas están dando cabal cumplimiento a todas las normas existentes relacionadas con el "hábeas data", tal y como lo estipula la Ley 1581 de 2012 y su correspondiente desarrollo reglamentario"*[14].

En relación a la anterior ley, también se menciona el Decreto 1704 de 2012 en el que se estipula la cantidad de tiempo que deben resguardar los prestadores de servicios de telecomunicaciones la información de sus suscriptores. Al respecto

[12] El Espectador. 11 de julio de 2015.
[13] El Espectador. 23 de julio de 2015.
[14] El Espectador. 20 de mayo de 2015.

vale la pena recordar que este decreto obliga a estas empresas a crear *backdoors* para facilitar la interceptación de comunicaciones al Estado, lo que significa que no es precisamente una ley que regule los procesos de vigilancia estatal. En esta lógica se puede dudar de que la cantidad de tiempo estipulada, que es de cinco años, no sea únicamente con fines de resguardo de información. Dentro de las noticias, se encuentra el siguiente recorte:

> *"Unas de las normas que rige este aspecto es el Decreto 1704 de 2012, que establece que los proveedores de redes y servicios de telecomunicaciones "deberán mantener actualizada la información de sus suscriptores y conservarla por el término de cinco años"[15].*

Respecto de la Ley 1621 de 2013 se habla bastante dentro de las noticias, al ser la Ley de Inteligencia que por el año 2015 daba tanto expectativas para el oficialismo. A pesar de este positivismo, Cortés Castillo (2014) sentan vacíos que dan pie a violaciones desde las actividades que desde los organismos de inteligencia se ejecutan. En cuanto a la Ley como tal, se encontraron los siguientes recortes:

> *"Con la ley de inteligencia que el Congreso aprobó en 2013, se creó la Comisión de Inteligencia que hoy preside el senador Carlos Fernando Galán, de Cambio Radical. "Durante mucho tiempo los aparatos de inteligencia del país operaron sin un marco legal apropiado; la ley 1621 de 2013 no solo pretende superar estos problemas sino establece el control político en cabeza del Congreso"[16].*

> *"En el espectro de las actividades de inteligencia y contrainteligencia la cosa no cambia mucho, pues allí, la Ley 1621 de 2013 establece que los operadores están obligados a "suministrar a los organismos de inteligencia y contrainteligencia, previa solicitud y en desarrollo de una operación autorizada y siempre que sea técnicamente viable, el historial de comunicaciones de los abonados telefónicos vinculados, los datos técnicos de identificación de los suscriptores sobre los que recae la operación, así como la localización de las celdas en que se encuentran las terminales y cualquier otra información que contribuya a su localización"[17].*

> *"Luego se creó una Ley de Inteligencia (1621 de 2013) y, a través de ella, una comisión de ocho congresistas para ejercer control y evitar que se repitieran situaciones similares. Hace unos meses, en entrevista con este diario, su primer presidente -el senador Carlos Fernando Galán- admitió que "durante mucho tiempo los aparatos de inteligencia de este*

[15] El Espectador. 20 de mayo de 2015.
[16] El Espectador. 18 de julio de 2015.
[17] El Espectador. 20 de mayo de 2015.

*país operaron sin un marco legal apropiado". El lío es que la comisión nunca ha podido funcionar"*[18].

Durante 2016 se dio a luz el nuevo Código de Policía, el cual dentro de las noticias seleccionadas lleva más críticas que elogios, en lo que respecta al derecho a la privacidad, un signo más de que lo que se legisla públicamente en Colombia no se da en razón del bien público y el respeto a los derechos humanos. Se encontraron los siguientes recortes:

*"Este código [de policía], entre muchas perlas, parece confundir la privacidad con el domicilio, y considera que los bienes que se encuentren en un espacio público no son privados. Desde estas premisas, se permite la intervención policial para acceder a la información y datos recolectados en estos espacios. Es decir, que quien vaya caminando con su celular por una calle, tendría que renunciar a la intimidad de sus conversaciones, chats o, en general, los contenidos que aparezcan en sus teléfonos, tabletas y computadores"*[19].

*"Y por último recordó que tanto el Código Nacional de Policía como la Ley de Inteligencia debían cumplir con el Pacto Internacional de Derechos Civiles y Políticos, que protege la vida privada, la familia, el domicilio y la correspondencia"*[20].

Igualmente durante el 2016 el Consejo Nacional de Política Económica y Social (CONPES) estaba trabajando en una nueva política de seguridad digital. Si bien este desarrollo se daba en un momento preciso para dar respuesta a diferentes problemáticas que con la era digital se fueron dando y profundizando, se encontraron fallas en los borradores expuestos por el CONPES y que se hicieron saber en la prensa. Sin embargo, también se daba mucha expectativa a la política en función de la ciberseguridad y la ciberdefensa nacional; a continuación algunos recortes al respecto:

*"El nuevo Conpes llega cinco años después de su antecesor (3701 de 2011), que impulsó la Ley de Inteligencia, así como la creación de instituciones para la ciberseguridad, principalmente en el sector defensa. El documento actual, en parte, continúa por esta línea y propone el establecimiento de varias entidades o cargos relacionados con el tema: consejero presidencial para la Seguridad Digital, Centro Criptológico Nacional, Centro de Excelencia Nacional de Seguridad Digital, Centro Nacional de Protección y Defensa de Infraestructura Critica Nacional, y la instalación de un enlace en cada Ministerio y Departamento Administrativo para entenderse con el Gobierno Nacional en materia de seguridad digital. El texto también*

[18] El Espectador. 12 de diciembre de 2015.
[19] El Espectador. 11 de noviembre de 2016.
[20] El Espectador. 11 de noviembre de 2016.

*propone actualizar la Ley de Inteligencia y Contrainteligencia "con el fin de enmarcar las actividades relacionadas con la seguridad digital, haciendo énfasis en la Ciberseguridad y la Ciberdefensa"[21].*

*"Dentro de los principios que establece el Conpes se encuentra "salvaguardar los derechos humanos y los valores fundamentales de los individuos, incluyendo la libertad de expresión, el libre flujo de información, la confidencialidad de la información y las comunicaciones, la protección de los datos personales y la privacidad (...)"[22].*

*"... un avance que el documento sobre seguridad digital abordara dos grandes enfoques: prosperidad social y económica y otro de la defensa nacional y la persecución al crimen. Es positivo que no sea sólo un texto pensado para la criminalidad en entornos digitales"[23].*

*"Nos preocupa que el Conpes se olvidó de que en Colombia el Estado también tiene que ser tenido en cuenta como un actor de la seguridad y la inseguridad digital. El documento olvida por completo el tema de las chuzadas o de Hacking Team. Las facultades de vigilancia del Estado no tienen los controles adecuados. Hay menciones de temas como phisiging, robos de identidad y esto es importante, pero lo otro también lo es"[24].*

*"Echamos de menos que algunos de los principales incidentes de seguridad digital en Colombia han tenido que ver con injerencias arbitrarias ilegales por parte de organismos de seguridad del Estado. Extrañamos que esto no hiciera parte de los casos que figuran como antecedentes de la política"[25].*

Se encuentra en general una desazón respecto a las leyes desarrolladas en función de la seguridad y privacidad de la ciudadanía en Colombia, declarándolas como débiles, poco claras, excesivas, entre otras. Al respecto se resaltan los siguientes recortes:

*"Más allá de la comisión creada por el gobierno Santos o las preliminares del ente investigador, una vez más queda en evidencia que el control sobre los servicios de inteligencia del país es débil o, peor, inexistente"[26].*

*"Revisamos los sistemas que la Dipol ha construido y encontramos que usan herramientas en la sombra, sistemas que no conoce el público en Colombia y que no tienen salvaguardas legales claras que impidan su abuso"[27].*

*"La opinión entre varios expertos es que el panorama legal del país en este aspecto [respecto al tratamiento datos personales] es vago y confuso"[28].*

---

[21] El Espectador. 4 de febrero de 2016.
[22] El Espectador. 4 de febrero de 2016.
[23] El Espectador. 4 de febrero de 2016.
[24] El Espectador. 4 de febrero de 2016.
[25] El Espectador. 4 de febrero de 2016.
[26] El Espectador. 9 de diciembre de 2015.
[27] El Espectador. 29 de agosto de 2015.
[28] El Espectador. 20 de mayo de 2015.

> *"… ha dicho que el término de retención de datos en el país es excesivo y pone a la ley colombiana como una de las "más draconianas en el mundo: no tiene comparación en la región y sí va a la par de países como China"*[29]*.*
>
> *"... en estas leyes "Hay bastante ambigüedad en un tema en el que de por medio están los derechos fundamentales de todos"*[30]*.*
>
> *"... pero es que así no funcionan las leyes. Deben ser explícitas, públicas y las deben entender los ciudadanos. De lo contrario no podríamos comprender de manera efectiva qué están haciendo las agencias y de qué son capaces, y este es un panorama aterrador"*[31]*.*
>
> *"Si bien la interceptación de comunicaciones bajo orden judicial está regulada en todos los países, con mayores o menores salvaguardas, esta no es suficiente pues el software de Hacking Team es mucho más invasivo que una mera interceptación… Como esto no es parte de la legislación, dudosamente es parte del orden judicial, por lo que el derecho al debido proceso también se ve vulnerado"*[32]*.*

Se sugiere en un recorte que las normativas de vigilancia de las comunicaciones sean necesarias, proporcionales y legítimas, lo cual va directamente relacionado a lo propuesto por la Electronic Frontier Foundation (2014) en los principios internacionales en la aplicación de derechos humanos a la vigilancia de comunicación:

> *"Por eso debemos asegurarnos que las normativas de vigilancia de las comunicaciones son necesarias, proporcionales y legítimas y que cuentan con las garantías legales que permitan la supervisión publica, la rendición de cuentas, mayor transparencia y así se evite el abuso de poder por parte del Estado"*[33]*.*

Esto es precisamente la sugerencia más pertinente para estos casos de vigilancia, pues con estos principios se asegura una vigilancia responsable y dirigida a grupos específicos de personas, no masiva.

Por último, dentro de esta subcategoría de "Ley" vale la pena incluir una subcategoría que sería la de transparencia, la cual es constantemente mencionada dentro de la prensa, en relación a la adquisición y uso de sistemas de vigilancia. Transparencia en este caso se refiere a que todas las acciones hechas por los

[29] El Espectador. 20 de mayo de 2015.
[30] El Espectador. 20 de mayo de 2015.
[31] El Espectador. 29 de agosto de 2015.
[32] El Espectador. 5 de septiembre de 2016.
[33] El Espectador. 17 de mayo de 2016.

Estados deben ser fácilmente conocidas por cualquier ciudadano, y por tanto documentadas públicamente; ha sido demostrado que no es así en Colombia con los sistemas de vigilancia, ya que se les conoce en la sombra (Privacy International, 2015b), a escondidas de la ciudadanía han dado a conocer en escándalos como el caso de Hacking Team (Pérez de Acha, 2016). Se destacan los siguientes recortes:

> *El tercer problema es la falta de transparencia y ética de Hacking Team por vender a países que luego chuzan a periodistas y opositores, lo que ya había sido detectado por dos informes de la Universidad de Toronto"*[34]*.*
>
> *"Citizen Lab resaltó otro aspecto importante: "La combinación de la proliferación global, y las promesas dudosas de sigilo, lleva a posibles peligros en un mercado sin regulación y sin transparencia"*[35]*.*
>
> *"En este sentido debe existir mayor transparencia en el uso y adquisición de estas herramientas, unaiscusión abierta sobre los estándares que deben regir esta tecnología y además sanciones penales en los casos que lo ameriten"*[36]*.*

### 4.3. Gobierno involucrado en la gestión y control de sistemas de vigilancia

Se menciona la subcategoría gobierno para encontrar instituciones oficiales involucradas (o que debiesen estarlo, por sugerencias dadas en las noticias) en los procesos de gestión y control de los sistemas de vigilancia estatal. De los primeros mencionados es la Procuraduría la cual debe estar como ente de control de los sistemas de vigilancia, considerando su tendencia a poner en duda la privacidad de la ciudadanía; se encuentran los siguientes recortes:

> *"El siguiente organismo en la lista es la Procuraduría, a la que le piden que investigue si los oficiales de la DIJIN y la DIPOL que adquirieron los sistemas de vigilancia, como PUMA y el IRS, lo hicieron dentro del marco legal colombiano y que publiquen el resultado de su trabajo"*[37]*.*
>
> *"... la organización hace una lista de sugerencias a los principales organismos involucrados en esta polémica y a entes de control como la Procuraduría y la Superintendencia Delegada para la Protección de Datos Personales"*[38]*.*

[34] El Espectador. 10 de julio de 2015.
[35] El Espectador. 11 de julio de 2015.
[36] El Espectador. 5 de septiembre de 2016.
[37] El Espectador. 30 de agosto de 2015.
[38] El Espectador. 30 de agosto de 2015.

La Fiscalía es otro de los llamados, sino el principal, a cumplir su rol de control sobre los sistemas de vigilancia estatal, y así se ha hecho saber dentro de la prensa. En la ley, la Fiscalía es el único ente gubernamental con los permisos para habilitar una interceptación, por tanto se le toma en cuenta para la toma decisiones al respecto que se hagan a nivel estatal desde cualquier institución pública. Así se puede ver en los siguientes recortes:

> *"Primero, cuando los medios informaron sobre Puma, la propia Policía salió a decir que no tenía fines de inteligencia, que era una estrategia para enfrentar a la delincuencia común, bajo supervisión de la Fiscalía"*[39].

> *"Sin embargo, hasta el momento, ni el director de esa institución, general Rodolfo Palomino, ni el gobierno Santos se ha pronunciado al respecto para confirmar o negar el dato. Lo relevante, además del hallazgo periodístico en sí mismo, es que si la compra de tal software se realizó, esa adquisición no fue informada al público porque correspondería a un movimiento de seguridad nacional que estaría cubierto por el secreto, o porque es un negocio que no está dentro de los parámetros legales. La Fiscalía General, única entidad autorizada para interceptar comunicaciones, dirá la última palabra"*[40].

> *"El Espectador le preguntó a la Fiscalía quién ejerce control sobre sus salas de interceptación. La respuesta fue que, cada mes, el director del CTI hace una auditoría en la que se revisa que lo que se está interceptando corresponda con lo que han aprobado los jueces. En la Policía, se supone -el general Palomino podría explicar mejor-, también hay controles internos"*[41].

> *"A la Fiscalía, por otra parte, le recomiendan que tenga en cuenta los antecedentes de la forma en que el DAS desarrolló las "chuzadas" a través de su propio sistema de monitoreo, llamado Esperanza"*[42].

Vale la pena destacar que, en julio de 2015, el fiscal general de la Nación, Eduardo Montealegre dio a conocer su férrea posición frente a PUMA, deshabilitándolo por sus alcances técnicos en la interceptación masiva de comunicaciones, y dejando claro que la única entidad gubernamental que puede hacer cualquier tipo de interceptación es la Fiscalía misma. Se resaltan los siguientes recortes:

> *"Pero Puma no está funcionando. De hecho, no pudo arrancar por una feroz oposición del fiscal general, Eduardo Montealegre, quien señaló que Puma podía volverse una rueda suelta y que sólo la Fiscalía tenía la facultad de interceptar comunicaciones"*[43].

[39] El Espectador. 10 de julio de 2015.
[40] El Espectador. 25 de julio de 2015.
[41] El Espectador. 18 de julio de 2015.
[42] El Espectador. 30 de agosto de 2015.

> *"Estas aseveraciones se prestaron para un sainete en el que el fiscal Montealegre evidenció la incompatibilidad con la plataforma para interceptaciones Esperanza y dijo con buen tino que Puma se prestaba para abusos, que no era necesaria y que aumentaba la intranquilidad de las personas"*[44].

Otro de los entes de control es la Corte Constitucional que pareciera haber fallado en su análisis a la Ley de Inteligencia, siendo un ejemplo más de que los avances en tecnología no logran ser alcanzados por la Constitución, dejando sin herramientas eficaces a los legisladores y tomadores de decisión en la Corte a optar por análisis más avanzados y pertinentes respecto a temas como el de vigilancia estatal y masiva. Se destaca el siguiente recorte:

> *"De otra parte, si la Corte hubiera conocido esa capacidad cuando analizó la constitucionalidad de la ley de inteligencia ¿habría fallado igual? Pareciera que aunque durante la revisión constitucional, varios académicos, ONG y entes del Estado (como la Defensoría del Pueblo) advirtieron problemas, el análisis de la Corte fue pensando en "pinzas de cocodrilo" más que en las actuales capacidades tecnológicas"*[45].

En la prensa también se encuentra a la Dirección de Inteligencia de la Policía Nacional la cual es pieza clave en todo el tema de contratación, gestión y administración de los diferentes sistemas de vigilancia estatal y masiva (este apartado se profundiza en la Subcategoría III.7. Policía y milicia). Se encuentran recortes como el siguiente:

> *"... el Gobierno colombiano, a través de la Dirección de Inteligencia de la Policía Nacional, parece ser uno de los compradores estrella, ya que aparecen pagos atribuidos a Puma, la plataforma de vigilancia de las comunicaciones que ya había sido cuestionada en el 2013. La información filtrada evidencia problemas de orden político, jurídico y ético tanto para Colombia como para Hacking Team"*[46].

### 4.4. Ciudadanía, derechos humanos y vigilancia estatal

En esta sección se construye un discurso en el que la ciudadanía, esperando que la fuerza pública haga todo lo posible por mantener la seguridad y el orden, se ve

---

[43] El Espectador. 11 de julio de 2015.
[44] El Espectador. 10 de julio de 2015.
[45] El Espectador. 3 de septiembre de 2015.
[46] El Espectador. 10 de julio de 2015.

afectada en sus derechos y debe optar por herramientas de defensa contra su propio Estado. Se encuentran así los siguientes recortes:

> *"En un país como éste, que la Fuerza Pública recurra a todas las herramientas posibles para combatir el crimen es lo mínimo que los ciudadanos esperan"*[47].

> *"... la Policía diría en un comunicado que "el objetivo de la adquisición de esta herramienta fue la protección de los colombianos"*[48].

> *"No se habla de contrataciones para combatir la delincuencia y la criminalidad, sino de espías a ciudadanos… El gobierno, en lugar de proteger y garantizar los derechos de los ciudadanos, los viola de manera flagrante."*[49].

> *"... la normativa de inteligencia no contempla la notificación a los usuarios de la realización de actividades de vigilancia de las comunicaciones en su contra (...). En otras palabras, en Colombia una persona no puede consultar si existen o han existido en el pasado acciones de inteligencia en su contra, ni pedir su corrección, ni hay un juez que controle la realización de ciertas actividades de inteligencia que inciden en sus derechos fundamentales"*[50].

> *"Lo que falta es, primero, que los ciudadanos asuman que tienen el derecho a proteger sus comunicaciones"*[51].

> *"Frente a las vejaciones de los poderes fuertes, el control de la información se ha vuelto una tarea del ciudadano en el cumplimiento de sus deberes democráticos"*[52].

Por esto, la ciudadanía colombiana tiene una fuerte desconfianza en el Estado respecto a los temas de vigilancia, afirmación que se destaca en el siguiente recorte:

> *"Colombia ha construido una amplia capacidad de vigilancia --recordemos la adquisición de herramientas como las de "Hacking Team"-- y no ha creado límites y controles a pesar de que el abuso de esa capacidad es noticia frecuente. La ausencia de esta perspectiva contribuye a la desconfianza de la ciudadanía que cree que el Estado suele aprovechar toda tecnología a su alcance para vigilar…"*[53].

A pesar de esta realidad en la que los ciudadanos se ven afectados en otros ámbitos, en razón de la seguridad que el Estado le debe cerciorar, se destacan voces en las que se afirma que puede haber otras salidas o estrategias de vigilancia y seguridad que no afecten los derechos fundamentales de la ciudadanía:

---

[47] El Espectador. 11 de julio de 2015.
[48] El Espectador. 11 de julio de 2015
[49] El Espectador. 22 de julio de 2015.
[50] El Espectador. 20 de mayo de 2015.
[51] El Espectador. 26 de julio de 2015.
[52] El Espectador. 13 de agosto de 2015.
[53] El Espectador. 18 de agosto de 2016.

*"La seguridad nacional y la privacidad no se excluyen mutuamente. Ambas pueden lograrse a través de la recolección responsable de inteligencia, que respete las libertades de los ciudadanos que siguen la ley"*[54].

*"Aunque el desarrollo de las tecnologías avanza más rápido que el derecho, existen principios para que estas herramientas no vulneren la libertad y dignidad de los ciudadanos"*[55].

## 4.5. Proceso de Paz y vigilancia estatal

Como en páginas anteriores se mencionaba, el proceso de paz durante 2015 y 2016 estaba en sus fases final de diálogo y votación, por lo que se decide habilitar la subcategoría de paz y conocer cómo los sistemas de vigilancia estatal intervienen en el mismo. Se encuentra que los periodistas han sido objetivos de vigilancia por el cubrimiento que han hecho al proceso de paz, siendo una muestra más de que afectan los derechos de libertad de expresión y asociación (Organización de las Naciones Unidas, 2014):

*"De acuerdo con las investigaciones hay otros periodistas interceptados ilegalmente, entre ellos, Jairo Lozano y Slobodan Wilches, de la FM, el columnista Daniel Coronell y la periodista de este diario y del programa Los Informantes, María del Rosario Arrázola, reconocida, entre otras, por el cubrimiento que ha hecho de las negociaciones de paz entre el gobierno y las Farc en La Habana (Cuba)"*[56].

*"De acuerdo al informe "Manual Antiespías" de la Fundación, durante el 2014 la Fiscalía General reveló que los periodistas "han sido vigilados en virtud de su actividad", por lo que se cree que más de un centenar de comunicadores fueron vulnerados, la mayoría por cubrir el proceso de paz"*[57].

También se hacen sugerencias a la Política de Seguridad Digital en diseño por el Consejo Nacional de Política Económica y Social (CONPES), encontrando de más interesante que se han sugerencias en pro del posconflicto y justicia transicional, dos conceptos claves para el proceso de paz, y que deben incluirse para pensar en la implementación de los sistemas de vigilancia estatal, algo que sería realmente innovador para los estudios en vigilancia. Se resaltan los siguientes recortes:

[54] El Espectador. 3 de junio de 2015.
[55] El Espectador. 22 de julio de 2015.
[56] El Espectador. 4 de diciembre de 2015.
[57] El Espectador. 9 de diciembre de 2015.

*"Dados los antecedentes de Colombia, sería importante que existiera un énfasis en los temas de posconflicto y justicia transicional en la política de seguridad digital"*[58].

*"Otra de las recomendaciones de los observadores tiene que ver con que el documento "no se hace pensando en una clave de posconflicto. No se va a hacer ciberdefensa y ciberseguridad en clave de combatir a un enemigo en un conflicto armado, sino a bandas criminales en una instancia", dice Vargas, de la Flip"*[59].

### 4.6. Vigilancia estatal, democracia y esfera pública

A pesar de que es poco mencionada en la prensa seleccionada, la democracia se resalta como una subcategoría relevante a este trabajo, en tanto es la forma de vida política que constitucionalmente se ejerce en Colombia y se querían encontrar relaciones o divergencias con la vigilancia estatal y masiva. Stahl (2016) discierne sobre la relación entre vigilancia estatal masiva y democracia, tomando como fundamento el concepto de esfera pública de Habermas, en la que destaca que dicha vigilancia hace imposible a los ciudadanos controlar las relaciones constitutivas de sus discursos, haciendo imposible la creación orgánica de colectivos; esto conlleva a una forma de ejercicio de poder político sobre la esfera pública que es incompatible con la idea de la autodeterminación democrática.

Es importante resaltar esta relación, más allá de que parezca lógica a las afirmaciones hasta ahora alcanzadas o citadas. Al respecto, por ende, se muestran los siguientes recortes:

*"En palabras de Ian Brown, profesor del Instituto de Internet de Oxford, "lo que Snowden nos ha dado es una elección: ¿creemos, como sociedad, que las amenazas que los gobiernos invocan para justificar estos programas de vigilancia en efecto los justifican, y por cuánto tiempo?¿Renunciar a la información personal y esperar que nuestros datos los manejen sabiamente las autoridades es el precio de la era digital?¿O creemos que hay mucho riesgo de abuso en la vasta cantidad de información privada que producen estas actividades, y que en estos riesgos no sólo se juega la privacidad de los ciudadanos, sino los derechos humanos y la democracia, como para permitir que este sistema siga operando?"*[60].

*"En el evento en que se llegara a comprobar que existe relación entre los hechos denunciados y los seguimientos e interceptaciones considero que estaríamos frente a un hecho muy grave*

[58] El Espectador. 4 de febrero de 2016.
[59] El Espectador. 4 de febrero de 2016.
[60] El Espectador. 6 de octubre de 2015.

*que atenta contra la democracia y la libertad de prensa", sostuvo el jefe del ente investigador el pasado 3 de diciembre"*[61].

[61] El Espectador. 4 de diciembre de 2015.

## CAPÍTULO V. Vigilancia estatal y privacidad de la ciudadanía en la prensa escrita digital en Colombia.

Desde las categorías de *Framing* y *Agenda setting* se realizan dos análisis principalmente: el primero, con características cuantitativas, muestra las categorías más mencionadas en el corpus de noticias elegido teniendo en cuenta que constituyen una guía sobre los temas con mayor presencia en la agenda de los medios; y el segundo, resalta aquellas categorías que llaman la atención acerca de cómo se tratan los temas de vigilancia estatal y de privacidad de la ciudadanía.

A continuación, se muestran las categorías con mayor mención dentro del corpus de noticias:

| Posición | Frecuencia | Categoría |
|---|---|---|
| **1** | 214 | policía |
| **2** | 196 | vigilancia |
| **3** | 172 | información |
| **4** | 159 | seguridad |
| **5** | 155 | derecho |
| **6** | 131 | país |
| **7** | 128 | empresa |
| **8** | 119 | comunicación |
| **9** | 116 | inteligencia |
| **10** | 112 | gobierno |
| **11** | 107 | colombia |
| **12** | 106 | dato |
| **13** | 100 | público |
| **14** | 88 | masivo |
| **15** | 88 | tratado-ley |
| **16** | 82 | herramienta |
| **17** | 81 | software |
| **18** | 81 | tecnología |
| **19** | 79 | nacional |

| | | |
|---|---|---|
| **20** | 72 | documento |

De estas categorías es relevante destacar aquellas que representan mayor interés para el campo de estudio de vigilancia y privacidad, a conocer:

- **Policía:** Es una categoría central para el estudio de vigilancia estatal y privacidad en Colombia al ser la principal imagen de fuerza pública en el país que se encarga de estos temas y a la cual se le cuestiona al respecto.

- **Seguridad:** Es la razón de interés en la mayoría de estudios de vigilancia por ser su principal movilizante y causal; la vigilancia sin la seguridad, no representaría tanta importancia en la discusión pública como lo hace ahora.

- **Derecho:** Llama la atención que se habla bastante de los derechos humanos y de cómo estos están siendo afectados por los sistemas de vigilancia, siendo el más mencionado el de privacidad.

- **Empresa:** Esta categoría es importante porque en los acercamientos que se han hecho sobre vigilancia en Colombia, la relevancia que llevan las empresas encargadas de la venta y distribución de los sistemas de vigilancia estatal y masiva es comprensible en tanto se relaciona directamente a los recursos públicos y a los procesos de contratación realizados (principalmente a escondidas de la ciudadanía).

- **Inteligencia:** Esta es una categoría emergente y se constituye como un pilar fundamental para estudiar la vigilancia estatal.

- **Tecnología, software, herramienta:** Al estar inmersos en temas de tecnología y lo digital, estas categorías son fundamentales para no dejar de lado los acercamientos técnicos que posibiliten análisis más precisos respecto a los alcances de los diferentes sistemas.

El resto de categorías como vigilancia, información, comunicación, etc. se dan por simples razones de mención. Para ver el listado de palabras completo, se puede ver el Anexo IV.

En este apartado también es importante resaltar que el periódico El Espectador presenta 69 noticias y El Tiempo 14 noticias relacionadas a los temas de vigilancia estatal y privacidad de información. No sólo cuantitativa sino cualitativamente, El Espectador presenta una agenda con mayor interés en los temas relacionados, con mayor profundidad en el caso nacional y tomando como referencia casos extranjeros; El Tiempo, a diferencia, presenta vagamente el caso de PUMA y un caso no asumido por El Espectador en Francia, donde se posibilita a la Agencia de Inteligencia de este país a intervenir comunicaciones sin la necesidad de un juez.

Se puede afirmar que los temas de vigilancia estatal y privacidad de información si cuentan con un espacio en la agenda de El Espectador, con un tratamiento desde diferentes puntos de vista sociales, económicos, jurídicos y legales, demostrando un esfuerzo de exhaustividad dejando al lector información clara con la ayuda de varios expertos en estos temas.

A continuación, se muestran aquellas categorías que llaman la atención acerca de cómo se tratan los temas de vigilancia estatal y de privacidad de la ciudadanía en la prensa elegida.

### 5.1. El escándalo de la vigilancia estatal

Los temas de vigilancia estatal en la mayoría del mundo se han visto envueltos en casos de escándalo, y Colombia no es una excepción, así lo hizo saber Privacy International (2015b), donde concluye que "los organismos están creando sus propios sistemas de vigilancia en la sombra, sin escrutinio suficiente ni base legal". Esto demuestra que la prensa se constituye como un medio en el que se dan a conocer estos secretos de Estado, que son problemáticos en la medida que son

sistemas que afectan directamente la privacidad de la ciudadanía, entre otros derechos. Se destacan los siguientes recortes al respecto:

> *"Lo relevante, además del hallazgo periodístico en sí mismo, es que si la compra de tal software se realizó, esa adquisición no fue informada al público porque correspondería a un movimiento de seguridad nacional que estaría cubierto por el secreto, o porque es un negocio que no está dentro de los parámetros legales"*[62].
>
> *"Pero no porque era un derecho de los ciudadanos saber si el Estado planeaba vigilarlos ilegalmente o incumplir con la Constitución, sino más bien porque la información no se podía considerar secreto de Estado"*[63].
>
> *"Si es cierto, como parece, el escándalo de vigilancia masiva de la NSA gringa pasa a gobiernos latinoamericanos (Chile, Colombia, Ecuador, Honduras, México y Panamá aparecen como clientes) al confirmarse que pueden espiar agresivamente; nada proporcional o necesario"*[64].
>
> *"Unos dicen que el dilema no existe, que para protegernos el Estado no puede mantener el secreto porque cualquier otro también puede usar esa falla de seguridad"*[65].
>
> *"Se descubrió que personal de la Dirección de Inteligencia de la Policía Nacional (Dipol) grababa de manera ilegal a miembros del Gobierno, de la oposición y periodistas desde hacía dos años", señaló entonces la propia revista. El escándalo le costó la cabeza a 11 generales, incluido el director de la época, Jorge Daniel Castro"*[66].

En este último recorte se destaca que, a pesar de que hay consecuencias directamente en el personal de la institución pública, se da luego de conocer un historial bastante amplio de vigilancia selectiva y masiva en Colombia que no resulta en efectos realmente visibles para el beneficio de la ciudadanía.

### 5.2. Amenazas de la vigilancia estatal

La otra cara muestra como amenaza a los sistemas de vigilancia estatal y masiva que, al ser desproporcionales e innecesarios en muchas ocasiones, pueden causar más males que beneficios; en este aparte han sido claros los principios planteados por la Electronic Frontier Foundation (2014) en donde proponen una vigilancia e interceptación de comunicaciones proporcional, necesaria y legítima,

[62] El Espectador. 25 de julio de 2015.
[63] El Espectador. 13 de agosto de 2015.
[64] El Espectador. 10 de julio de 2015.
[65] El Espectador. 18 de agosto de 2016.
[66] El Espectador. 11 de julio de 2015.

correspondiente a un contexto particular y no masivo, preferiblemente. Se muestran a continuación los recortes mencionados:

> *"¿Cuáles son las consecuencias que la vigilancia masiva tiene para los ciudadanos? La amenaza de estar sujeto a este tipo de vigilancia sin sospechas bien fundadas es algo que cambia el comportamiento humano: la forma como actuamos, hablamos y nos comunicamos. Este efecto de la vigilancia es algo que pone en peligro derechos legítimos de las personas"*[67].

> *"En palabras de Ian Brown, profesor del Instituto de Internet de Oxford, "lo que Snowden nos ha dado es una elección: ¿creemos, como sociedad, que las amenazas que los gobiernos invocan para justificar estos programas de vigilancia en efecto los justifican, y por cuánto tiempo?"*[68].

> *"Para cuidar el crecimiento de la educación y el desarrollo que internet promueve, tenemos que estar atentos a las principales amenazas regionales: el espionaje indiscriminado (como vimos en el caso de Hacking Team)"*[69].

### 5.2.1. Respuesta de la vigilancia estatal a las amenazas

En esta subcategoría se encuentra una doble perspectiva respecto a los sistemas de vigilancia estatal. Una en la que la vigilancia estatal es una de las primeras respuestas a atender para enfrentar amenazas terroristas y la criminalidad nacional y extranjera, como se muestra en los siguientes recortes:

> *"La respuesta de la entidad fue un comunicado en el que indicó que "el propósito de esta compra fue potencializar la capacidad de detección de amenazas del terrorismo y la criminalidad organizada en el ciberespacio"*[70]

> *"En su momento, aún con los restos de las Torres Gemelas en televisión global, el auge de la amenaza del terrorismo extremista dio pie para la redacción de algunas de las leyes más drásticas en temas de vigilancia y seguridad"*[71].

> *"Poco más de una década después, el uso y el abuso de estas previsiones, redactadas y aprobadas bajo una amenaza tangible y aterradora, generaron uno de los mayores escándalos en el mundo de la vigilancia digital"*[72].

[67] El Espectador. 29 de agosto de 2015.
[68] El Espectador. 6 de octubre de 2015.
[69] El Espectador. 17 de mayo de 2016.
[70] El Espectador. 11 de julio de 2015.
[71] El Espectador. 18 de noviembre de 2015.
[72] El Espectador. 18 de noviembre de 2015.

## 5.3. Preocupación respecto a la vigilancia estatal

La muestra de preocupación sobre los temas de vigilancia estatal masiva se da principalmente en función de los derechos humanos que acarrea su ejecución. Ya lo hizo saber la Organización de las Naciones Unidas (2014) que la vigilancia afecta principalmente los derechos de privacidad, libertad de expresión y de asociación; los derechos humanos son la base de la convivencia en el mundo, por lo que su condición es fundamental para mantener un discurso que sopese el de la vigilancia estatal en razón de la seguridad. Se destacan los siguientes recortes:

> *"Javier Paello, analista de Access (una organización internacional que monitorea temas de derechos humanos en entornos digitales), le expresó a este diario su principal preocupación sobre "Galileo": "Las herramientas de HT son demasiado invasivas... Uno de los principios que se manejan en asuntos de vigilancia y derechos humanos es que las acciones deben ser necesarias y proporcionales, pero se vuelve muy complicado cuando son herramientas demasiado invasivas"*[73].

> *"La Relatoría Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos (CIDH) expresó, en un reciente pronunciamiento, su preocupación respecto a "una gran cantidad de información que indica que varios gobiernos del hemisferio habrían adquirido e implementado programas de vigilancia de las comunicaciones electrónicas que pueden generar un perjuicio serio a los derechos a la intimidad y a la libertad de pensamiento y expresión en la región"*[74].

> *"No es la primera vez que la Relatoría para la Libertad de Expresión manifiesta su preocupación por la utilización de programas de vigilancia masiva por parte de los Estados. Aunque el desarrollo de las tecnologías avanza más rápido que el derecho, existen principios para que estas herramientas no vulneren la libertad y dignidad de los ciudadanos"*[75].

> *"… una resolución de la Asamblea General de la ONU sobre "el derecho a la privacidad en la era digital", que menciona "una preocupación por la posible afectación del ejercicio y goce de DD.HH. por actos de vigilancia e interceptación de comunicaciones masivas o extraterritoriales, donde se exhorta a que los Estados actúen de forma respetuosa de aquellos derechos en el ámbito de internet"*[76].

> *"… una de las preocupaciones más grandes que deja su reporte es que la Dijín y la Dipol, dos ramas de inteligencia de la Policía, están buscando y comprando estos sistemas sin tener*

[73] El Espectador. 18 de julio de 2015.
[74] El Espectador. 22 de julio de 2015.
[75] El Espectador. 22 de julio de 2015.
[76] El Espectador. 22 de julio de 2015.

*ningún tipo de control por parte de la Fiscalía, el organismo colombiano que, por ley, debe liderar y filtrar las interceptaciones"*[77].

*"En el evento en que se llegara a comprobar que existe relación entre los hechos denunciados y los seguimientos e interceptaciones considero que estaríamos frente a un hecho muy grave que atenta contra la democracia y la libertad de prensa", sostuvo el jefe del ente investigador el pasado 3 de diciembre"*[78].

Respecto a la preocupación por la privacidad no hay mayor profundización, más allá de que está siendo afectada por los Estados de vigilancia, como se ven en los siguientes recortes:

*"En el mundo, hoy se habla del asunto con verdadera preocupación. Los expertos sostienen que el cambio sustancial actual es que la gente se ha dado cuenta del peligro que corre su intimidad y su privacidad"*[79].

*"Nos parece de la mayor preocupación porque este tipo de tecnología está diseñada para la intromisión en la privacidad a través de mecanismos digitales que permiten recolectar datos sin el conocimiento de las personas o instalar programas sin autorización en los dispositivos"*[80].

En la prensa se destaca también una preocupación sobre el uso de los recursos públicos y la transparencia que tienen los Estados cuando contratan y usan los sistemas de vigilancia, con la finalidad de que sean los ciudadanos que tengan la posibilidad de ejercer control sobre los gastos y acciones que hace su gobierno elegido democráticamente. Se destacan los siguientes recortes:

*"Esa es parte de nuestra preocupación y llamamos a los estados a que aporten más información. No basta con decir que los programas fueron adquiridos y se utilizan adecuadamente. Hay que explicar cuál es su alcance, qué tipo de intromisión en la privacidad suponen. Hay ciertos aspectos relacionados con la seguridad nacional que tienen que ser públicos"*[81].

*"Lo preocupante es que se utilizan recursos públicos en nuestra contra. El gobierno, en lugar de proteger y garantizar los derechos de los ciudadanos, los viola de manera flagrante. Lo más probable es que, pese a las evidencias, todo quede en la absoluta impunidad"*[82].

---

77 El Espectador. 30 de agosto de 2015.
78 El Espectador. 4 de diciembre de 2015.
79 El Espectador. 25 de julio de 2015.
80 El Espectador. 26 de julio de 2015.
81 El Espectador. 26 de julio de 2015.
82 El Espectador. 22 de julio de 2015.

## 5.4. Contexto de la vigilancia estatal y el tratamiento de datos en el extranjero

Vale la pena destacar que al estar los casos de vigilancia estatal vigentes en el período estudiado, en la prensa se evaluaron también casos del extranjero, en el que se destacan países como Estados Unidos, Paraguay y Francia, y el continente europeo. Esto funciona como método de comparación para reconocer buenas y malas prácticas en los temas relacionados. A continuación algunos recortes de referencia:

> *"[En Paraguay, el programa de vigilancia estatal] Daña derechos constitucionales como la privacidad, asociación y libertad de expresión, porque lo que propone esta ley es la vigilancia masiva de las personas, como si todas fueran culpables"*[83]
>
> *"El año pasado, Europa declaró inválida la directiva de retención de datos que había aprobado en 2006, por considerar que los plazos que establecía para capturar información de los ciudadanos (entre 6 y 12 meses) eran demasiado amplios"*[84].
>
> *"… la discusión en Paraguay ha estado mediada por el pulso entre la seguridad y la privacidad en la era digital, un asunto que fue expuesto con amplitud esta semana en la aprobación del Freedom Act en Estados Unidos, ley que, por primera vez en varias décadas, le impone límites a ciertas operaciones de vigilancia de los organismos de inteligencia de este país, particularmente la Agencia Nacional de Seguridad (NSA, en inglés)"*[85].
>
> *"También en Europa o Estados Unidos deberían empezar a preocuparse por el lamentable estado del cuarto poder, y por la batalla silenciosa de autoridades publicas y privadas, a punta de leyes y juicios, por el control de la vida privada de los ciudadanos y la circulación de la información"*[86].
>
> *"Lo que estamos viendo aquí, en nuestros gobiernos en Europa, es que la vigilancia masiva se está usando como un atajo a la hora de hacer trabajo de inteligencia y existe la idea de que entre más información exista, más fácil será filtrar a los criminales o a las personas de interés para las autoridades"*[87].
>
> *"… el deseo de los gobiernos de tener acceso preferencial a las tecnologías de encriptación no sólo debilitaría la seguridad de las comunicaciones modernas, sino también dañaría la*

[83] El Espectador. 10 de marzo de 2015.
[84] El Espectador. 20 de mayo de 2015.
[85] El Espectador. 3 de junio de 2015.
[86] El Espectador. 13 de agosto de 2015.
[87] El Espectador. 29 de agosto de 2015.

*infraestructura misma de internet. El reporte de los expertos señala en concreto a Estados Unidos y Reino Unido como dos de los países que más han perseguido esta agenda"*[88].

*"Una amplia mayoría de diputados franceses aprobaron este martes en primera lectura el proyecto de ley sobre los servicios de inteligencia, que autoriza la vigilancia de sospechosos sin pedir antes una autorización o el control de un juez"*[89].

## 5.5. Necesidad de la vigilancia estatal para la seguridad

Se evidencian diversos puntos de vista respecto a la necesidad de la vigilancia estatal para la seguridad, en lo que para este apartado lo que ofrece la Electronic Frontier Foundation (2014) respecto a los principios de la vigilancia de las comunicaciones con enfoque en los derechos humanos, sugiere que debe ser implementada solo cuando se le considere necesaria, de manera proporcional y, por ende, legítima, transparente. Así lo hace ver el siguiente recorte:

*"Por eso debemos asegurarnos que las normativas de vigilancia de las comunicaciones son necesarias, proporcionales y legítimas y que cuentan con las garantías legales que permitan la supervisión publica, la rendición de cuentas, mayor transparencia y así se evite el abuso de poder por parte del Estado"*[90].

Se encuentran igual posiciones totalmente positivistas respecto a la vigilancia estatal, en la que tomando como sustento la seguridad de la ciudadanía, en un mundo en que el terrorismo parece ser una de las más grandes preocupaciones de occidente, se justifica su existencia e inversión. Esto lo demuestra el siguiente recorte:

*"… la idea detrás de estas acciones [de vigilancia masiva], el sustento filosófico, por llamarlo de cierta forma: en el mundo del terrorismo la vigilancia masiva contra ciudadanos comunes y corrientes no sólo es conveniente, sino necesaria"*[91].

En su contraparte, se encuentran aseveraciones acerca de que la vigilancia estatal masiva es innecesaria principalmente por sus alcances que son muy invasivos por su diseño mismo:

---

[88] El Espectador. 18 de noviembre de 2015.
[89] El Tiempo. 6 de mayo de 2015.
[90] El Espectador. 17 de mayo de 2016.
[91] El Espectador. 3 de junio de 2015.

> *"Estas aseveraciones se prestaron para un sainete en el que el fiscal Montealegre evidenció la incompatibilidad con la plataforma para interceptaciones Esperanza y dijo con buen tino que Puma se prestaba para abusos, que no era necesaria y que aumentaba la intranquilidad de las personas"*[92].

> *"Uno de los principios que se manejan en asuntos de vigilancia y derechos humanos es que las acciones deben ser necesarias y proporcionales, pero se vuelve muy complicado cuando son herramientas demasiado invasivas"*[93].

Por lo mismo, se genera el debate central respecto a si una vigilancia estatal masiva puede ser proporcional (precisamente por su carácter masivo) y necesario, en la medida de si realmente es útil la información de personas no sospechas e inocentes con finalidades de seguridad e inteligencia. Esta duda la hace saber el siguiente recorte:

> *"La pregunta que acá persiste es si se pueden tener sistemas de vigilancia masiva que cumplan los requisitos de proporcionalidad y necesidad"*[94].

[92] El Espectador. 10 de julio de 2015.
[93] El Espectador. 18 de julio de 2015.
[94] El Espectador. 29 de agosto de 2015.

# CAPÍTULO VI. PRENSA DIGITAL Y VIGILANCIA ESTATAL: SUS PRINCIPALES ARISTAS

La aproximación que se hace a la vigilancia estatal es diversa en la prensa, y representa así mismo la multiplicidad de puntos de vista inter y multidisciplinares que convergen en su análisis. Se realizan acercamientos a sus características masivas, su relación a los derechos humanos, los procesos de adquisición, su congruencia con los procesos de inteligencia y contrainteligencia gubernamentales, y las tecnologías que son usadas para su funcionamiento, en un mundo de Internet; así mismo, se tratan los mecanismos de defensa que, como la encriptación, contrarrestan a la vigilancia estatal, principalmente para realizar actividades que requieren anonimato, como el ejercicio de prensa, de política, de investigación, entre otros. De la misma manera, se evidencia la relevancia histórica que tiene la fuerza pública en Colombia para los procesos de vigilancia estatal masiva y selectiva.

## 6.1. Vigilancia masiva

Entorno a las connotaciones sobre vigilancia masiva se asevera lo argumentado por Fuchs (2011) y Wall (2007), encontrando definiciones o acercamientos acerca del concepto como se ve en los siguientes recortes:

> *"En la práctica, lo que la retención masiva significa es la imposición sobre los operadores de telecomunicaciones de guardar los datos de actividad y tráfico de todos sus clientes"*[95].

> *"El problema con internet no es sólo la vigilancia masiva de gobiernos y agencias de inteligencia, la recolección indiscriminada de datos, metadatos, o la utilización de herramientas diseñadas para monitorear criminales, pero que terminan siendo usadas para rastrear a cualquiera, sospechoso tan sólo porque puede ser investigado"*[96]

[95] El Espectador. 10 de marzo de 2015.
[96] El Espectador. 14 de abril de 2015.

> *"... tecnología que está llegando al país está basada en un formato pasivo, es decir, que el sistema actúa como una gran red pescando en un mar de datos, exponiendo a cualquier ciudadano a que se invada su privacidad así no existan sospechas para hacerlo"*[97].

Parte de las formas de hacer vigilancia masiva es solicitar a las prestadoras de comunicaciones (empresas que ofrecen servicios de suscripción a telecomunicaciones, como Claro, Movistar, Virgin Mobile, DirecTV, etc.) acceso a la información que recolectan del tráfico de datos que sobrellevan. En este contexto, el recorte de prensa hace saber de su existencia:

> *"... por orden del gobierno, las empresas deben facilitar el acceso a sus redes y al contenido de sus usuarios, algo que no sólo vulnera a las personas, sino también a los protocolos de encriptación que hoy permiten buena parte de las comunicaciones seguras que son fundamentales para millones de clientes y para la red misma".*
>
> *"Esperanza", en cambio, está descrito como una plataforma que requiere que la Fiscalía contacte a un proveedor de comunicaciones para pedir información sobre un blanco específico: es un proceso activo de interceptación. Puma y el sistema de la Dipol son pasivos y están diseñados para la recolección y análisis de datos a gran escala"*[98].
>
> *"Otra petición al Senado es que revise si la obligación que tienen las operadoras de comunicaciones de guardar durante cinco años los datos que se interceptan, es apropiada"*[99].

Se encuentra en algunos recortes el menester de evaluar el alcance de la vigilancia masiva en cuanto a su proporcionalidad y necesidad, en relación al llamado de los 13 principios mencionados en "The International Principles on the Application of Human Rights to Communications Surveillance" (Electronic Frontier Foundation, 2014) que tiene como objetivo "clarificar cómo se aplica el derecho internacional de los derechos humanos en el actual entorno digital, en particular a la luz del aumento y de los cambios que están teniendo las tecnologías y técnicas de Vigilancia de las Comunicaciones". A continuación los recortes:

> *"La pregunta que acá persiste es si se pueden tener sistemas de vigilancia masiva que cumplan los requisitos de proporcionalidad y necesidad"*[100].

---

[97] El Espectador. 30 de agosto de 2015.
[98] El Espectador. 29 de agosto de 2015.
[99] El Espectador. 30 de agosto de 2015.
[100] El Espectador. 29 de agosto de 2015.

*"Además, en este país de leyes, se quejó el Comité por la redacción de la Ley de Inteligencia y Contrainteligencia que autoriza injerencias en las comunicaciones privadas con el monitoreo del espectro electromagnético sin un análisis de proporcionalidad"*[101].

*"el uso de programas o sistemas de vigilancia en las comunicaciones privadas debe estar establecido de manera clara y precisa en la ley, ser verdaderamente excepcional y selectivo, y estar limitado en función a lo estrictamente necesario para el cumplimiento de fines imperativos"*[102].

*"Por eso debemos asegurarnos que las normativas de vigilancia de las comunicaciones son necesarias, proporcionales y legítimas y que cuentan con las garantías legales que permitan la supervisión pública, la rendición de cuentas, mayor transparencia y así se evite el abuso de poder por parte del Estado"*[103].

## 6.2. Vigilancia y derechos humanos

Es también sabido que la vigilancia estatal trabaja desde un área gris en la que, en razón de la seguridad u otros propósitos, se pueden afectar las fronteras de los derechos humanos, principalmente aquellos propios de una democracia, como la libertad de expresión (Organización de las Naciones Unidas, 2014). Se destacan las menciones sobre la vigilancia a periodistas e inclusive a políticos:

*"Ahora todos esperan ser vigilados y se abstienen de expresar ciertas opiniones o afiliarse a un movimiento político determinado por miedo a ser espiados"*[104].

*"... han encontrado cómo el software de rastreo en línea ha sido vendido, sin restricciones ni condiciones, a países que, quizá, no lo usen para monitorear conductas criminales"*[105].

*"De acuerdo al informe "Manual Antiespías" de la Fundación, durante el 2014 la Fiscalía General reveló que los periodistas "han sido vigilados en virtud de su actividad", por lo que se cree que más de un centenar de comunicadores fueron vulnerados, la mayoría por cubrir el proceso de paz"* [106].

*"Debido a las recientes interceptaciones a periodistas en el país, la Fundación para la Libertad de Prensa (Flip) recordó cuáles son, al parecer, las aplicaciones utilizadas por las autoridades para realizar espionaje y les hizo un llamado para no olvidar que cualquier tipo de espionaje en las comunicaciones es considerado inconstitucional y viola la libertad de prensa"*[107].

---

101 El Espectador. 11 de noviembre de 2016.
102 El Espectador. 23 de julio de 2015.
103 El Espectador. 17 de mayo de 2016.
104 El Espectador. 4 de febrero de 2015.
105 El Espectador. 14 de abril de 2015.
106 El Espectador. 9 de diciembre de 2015.
107 El Espectador. 9 de diciembre de 2015.

*"Con este monitoreo, datos que se van a conservar por un año, se puede saber quién habla con quién, a qué hora, con quién se reúnen las personas; quiénes son las fuentes de un periodista, por ejemplo"*[108].

*"Así mismo señaló su preocupación, porque al parecer las interceptaciones que se están realizando desde inteligencia, no solo se están realizando a periodistas, sino además a sus familiares e hijos"*[109].

*"... maniobras que incluyeron la interceptación de las comunicaciones de la canciller alemana, Ángela Merkel, y la presidenta brasileña, Dilma Rousseff"*[110].

*"El tercer problema es la falta de transparencia y ética de Hacking Team por vender a países que luego chuzan a periodistas y opositores, lo que ya había sido detectado por dos informes de la Universidad de Toronto"*[111].

*"Cinco años atrás, en la era Uribe, HT ya había buscado hacer negocios con el DAS. Para esa época, se sabría después, en el Departamento Administrativo de Seguridad se interceptaban ilegalmente las comunicaciones de magistrados de altas cortes, periodistas, opositores y defensores de derechos humanos"*[112].

*El tipo de "malware" (software malicioso) que vende Hacking Team esencialmente hackea equipos para leer emails y mensajes incluso si esos mensajes nunca han sido enviados. Es una herramienta útil si se enfoca en los 'tipos malos', como narcotraficantes o pedófilos, con orden judicial. Pero es igual de mala si se usa contra periodistas, opositores…"*[113].

Se habla también de la integridad de las comunicaciones comprendiéndola dentro de este marco de derechos humanos y vigilancia, en convergencia con las leyes y la concientización por parte de la ciudadanía respecto a los derechos que se ven afectados. Al respecto, Cortés Castillo (2014) apunta que, en la búsqueda de un sistema de vigilancia balanceado, la regulación y la jurisprudencia deben conocer los alcances de las tecnologías de vigilancia masiva y las comparen con las garantías mínimas constitucionales y los derechos humanos. Se resaltan los siguientes recortes al respecto:

*"Ya en 2008 la Corte alemana señaló que no pueden usarse sin orden judicial y que la integridad de las comunicaciones es un derecho"*[114].

---

108 El Espectador. 10 de marzo de 2015.
109 El Espectador. 9 de diciembre de 2015.
110 El Espectador. 4 de febrero de 2015.
111 El Espectador. 10 de julio de 2015.
112 El Espectador. 18 de julio de 2015.
113 El Espectador. 18 de julio de 2015.
114 El Espectador. 23 de julio de 2015.

*"La protección efectiva del derecho a la privacidad debe provenir en parte de la creación de mejores leyes para evitar que las agencias de la Policía tengan la capacidad de interceptar información de manera masiva"*[115].

*"Lo que falta es, primero, que los ciudadanos asuman que tienen el derecho a proteger sus comunicaciones; segundo, que los estados promuevan el uso de estos mecanismos e informen sobre los mismos; tercero, una educación formal e informal que incorpore estos elementos"*[116].

## 6.3. Adquisición de tecnologías de vigilancia masiva

Es constante la mención en las diferentes noticias de la contratación/adquisición de las tecnologías de vigilancia masiva por parte del Estado Colombiano y por otros países mencionados como Francia, Ecuador, México, entre otros. Se destaca esta sección por el enfoque económico y ciudadano, en la medida que para la compra de estas tecnologías los recursos públicos son usados de manera secreta, y al mismo tiempo es la ciudadanía que devela toda esta información desde diferentes organizaciones sin ánimo de lucro como Privacy International o Datos Protegidos (Privacy International, 2015; Pérez de Acha, 2016).

*"Con base en las especificaciones técnicas que la Policía estaba pidiendo en un proceso de contratación. Además, sabemos que Verint, que fue el proveedor de esta tecnología, en su material de mercadeo asegura que tiene esa capacidad"*[117].

*"Según la información revelada, el Gobierno colombiano, a través de la Dirección de Inteligencia de la Policía Nacional, parece ser uno de los compradores estrella, ya que aparecen pagos atribuidos a Puma, la plataforma de vigilancia de las comunicaciones que ya había sido cuestionada en el 2013"*[118]

*"… la Policía diría en un comunicado que "el objetivo de la adquisición de esta herramienta fue la protección de los colombianos"*[119].

## 6.4. Vigilancia y comunicación

Cuando se hacen aproximaciones a la vigilancia masiva, se puede estar hablando al mismo tiempo de infraestructuras físicas con forma de panóptico, de cámaras de circuito cerrado, pero también de interceptaciones de comunicaciones. En el

[115] El Espectador. 30 de agosto de 2015.
[116] El Espectador. 26 de julio de 2015.
[117] El Espectador. 29 de agosto de 2015.
[118] El Espectador. 10 de julio de 2015.
[119] El Espectador. 11 de julio de 2015.

contexto del presente trabajo se apunta principalmente a este tipo de vigilancia y la relación que converge con la comunicación se torna más que relevante; desde una posición más crítica de la vigilancia como medio de dominación, como el mismo Fuchs (2011) menciona, también Lash (2007) afirma que ahora la dominación se da a través de la comunicación cada vez más inmediata y, cuando esto sucede, la soberanía y la democracia deben ser repensadas.

Se destacan algunas menciones de la interceptación de comunicaciones como centro de atención en las noticias analizadas:

> *"Colombia ha desarrollado un sistema de vigilancia de comunicaciones poco transparente y sin controles, ahora sabemos que también tienen capacidad de interceptación de comunicaciones a objetivos seleccionados que va más allá de PUMA (hablan de "Super PUMA" y presentan al desconocido SIGD de la DIPOL)"*[120].

> *"Y esto es especialmente complicado si se tiene en cuenta la historia colombiana sobre interceptaciones ilegales"*[121].

> *"... al mismo tiempo estamos en medio de la que probablemente es la revolución en comunicaciones más profunda en la historia de la humanidad"*[122].

> *"La amenaza de estar sujeto a este tipo de vigilancia sin sospechas bien fundadas es algo que cambia el comportamiento humano: la forma como actuamos, hablamos y nos comunicamos"*[123].

Se deja claro en algunos recortes que muchas veces de estas comunicaciones interceptadas no se recolectan y almacenan necesariamente sus contenidos sino principalmente sus metadatos (Mayer-Schonberger & Cukier, 2013), lo que demuestra una relevancia de este tipo de información que es en la mayoría de casos la que se obtiene en el tráfico de Internet en tanto no suelen estar protegidos como sí el contenido:

> *"… así cualquier pieza de legislación sobre el tema deja claro que no se solicitan los contenidos de las comunicaciones (la grabación de una llamada, por ejemplo), sino los metadatos de éstas: hora y fecha, lugar y direcciones IP (una especie de huella digital electrónica por la cual*

120 El Espectador. 3 de septiembre de 2015.
121 El Espectador. 29 de agosto de 2015.
122 El Espectador. 14 de abril de 2015
123 El Espectador. 29 de agosto de 2015.

*se sabe quién está a cada lado de la línea). El tema acá es que los metadatos a menudo revelan tanta (o hasta más) información sobre una comunicación"*[124].

A pesar de estas aseverciones, hay recortes que contradicen lo dicho, y la existencia de tecnologías enteramente intrusivas ya existen, por lo que las dudas respecto a este alcance permanecen al momento:

> *"Según los documentos de Hacking Team que se han filtrado, sus tecnologías de vigilancia son muy intrusivas y poderosas, van mucho más allá de la interceptación de comunicaciones y llegan hasta el "hackeo" de los dispositivos móviles de la gente, el acceso a todos sus archivos y toda su información. Para Privacy Internacional es preocupante que ese sea el nivel de acceso que la Policía está buscando tener"*[125].

### 6.5. Inteligencia como categoría emergente de la vigilancia estatal

Este concepto llama la atención al ser uno de los más mencionados entre todas las noticias. Se ha descubierto que hace parte de un lenguaje más legal que necesariamente académico y es necesario remontarse a un concepto de por sí más conocido como espionaje siendo una de las categorías fundamentales para la construcción de la inteligencia. El espionaje puede ser definido como el simple robo organizado de información, usualmente con fines militares y secretos gubernamentales (Khalil, 2015).

Inteligencia por ende tiende a ser una construcción más compleja que se le considera como el "producto de la colección, procesamiento, integración, evaluación, análisis, e interceptación de información disponible concerniente a naciones extranjeras, fuerzas o elementos hostiles o potencialmente hostiles, o áreas con operaciones hostiles" (Department of Defense, United States, 2017). De esta manera se puede establecer como una fuente de información al espionaje, y a la inteligencia como la encargada de interpretar tal información recolectada.

De inteligencia es válido ahondar en que se le divide en dos tipos: inteligencia foránea y contrainteligencia. La primera, entendida como la información

[124] El Espectador. 10 de marzo de 2015.
[125] El Espectador. 29 de agosto de 2015.

relacionada a las capacidades, intenciones o actividades de gobiernos o elementos foráneos; y la segunda, información recolectada, y actividades dirigidas, a protegerse del espionaje y otras actividades de inteligencia por personas u organizaciones internas, nacionales o foráneas que puedan resultar en sabotaje de actividades propias de inteligencia o relacionadas (Khalil, 2015).

Sin embargo, conceptualmente es evidente un traspasamiento de funciones entre espionaje, vigilancia e inteligencia en el ámbito de seguridad que se les enmarca. Es válido citar la definición que se le da desde el *Dictionary of military and associated terms* a vigilancia en donde se le delimita su función a "una observación sistemática del aero-espacio, ciberespacio, superficie, subterráneo, lugares, personas, o cosas específicas, por medios visuales, aurales, electrónicos, fotográficos, entre otros" (Department of Defense, United States, 2017).

La evidencia de la categoría de inteligencia se puede ver en los siguientes recortes:

> *"... el pulso entre el acceso a la información y la seguridad, entre la privacidad y las labores de inteligencia en un planeta aterrorizado, es una de las tensiones más importantes y necesarias a la hora de definir cómo será el crecimiento futuro de internet y con éste el de aquellos que hoy usan y usarán la red"[126].*
>
> *"La inteligencia informática es parte de la seguridad de la información. Se aplican herramientas tecnológicas para verificar y conocer datos sensibles que competen a la actividad que se desarrolle"[127].*
>
> *"El año pasado, la ONU les envió varias comunicaciones tanto a Hacking Team como al representante de Italia ante las Naciones Unidas preguntando por qué Hacking Team le había vendido el software RCS a Sudán, país que tenía un embargo de armas y que podía usar ese programa "para inteligencia militar electrónica"[128].*
>
> *"En EE. UU. este es un tema más asociado con la protección al consumidor, mientras que Europa tiende a asumirlo como un derecho fundamental. La diferencia no es un asunto semántico, pues a la larga esta división obliga a tomarse más, o menos, en serio la privacidad de los usuarios y a volverla más, o menos, permeable ante las labores inteligencia"[129].*

[126] El Espectador. 20 de mayo de 2015.
[127] El Espectador. 25 de julio de 2015.
[128] El Espectador. 11 de julio de 2015.
[129] El Espectador. 6 de octubre de 2015.

> *"... filtró documentos en los que mostraba cómo la Agencia Nacional de Seguridad de Estados Unidos (NSA, por sus siglas en inglés) estableció una red de vigilancia sobre las comunicaciones de millones de ciudadanos, una operación que realizó en conjunto con agencias de inteligencia de países como el Reino Unido"*[130].

> *"es clara la intencionalidad del gobierno de espiar a los ciudadanos. No se habla de contrataciones para combatir la delincuencia y la criminalidad, sino de espías a ciudadanos"*[131].

Se hace igual mención a los conceptos de inteligencia y contrainteligencia, como se ve en el siguiente recorte:

> *"En el espectro de las actividades de inteligencia y contrainteligencia la cosa no cambia mucho, pues allí, la Ley 1621 de 2013 establece que los operadores están obligados a "suministrar a los organismos de inteligencia y contrainteligencia, previa solicitud y en desarrollo de una operación autorizada y siempre que sea técnicamente viable…"*[132].

También se destaca que la vigilancia no siempre tiene por qué terminar en inteligencia, por lo que sí existe realmente una diferencia válida entre ambas categorías. Así lo hace ver el siguiente recorte:

> *"Lo que estamos viendo aquí, en nuestros gobiernos en Europa, es que la vigilancia masiva se está usando como un atajo a la hora de hacer trabajo de inteligencia y existe la idea de que entre más información exista, más fácil será filtrar a los criminales o a las personas de interés para las autoridades"*[133].

## 6.6. Encriptación como estrategia política y técnica de defensa a la vigilancia

Es llamativo también que las noticias no se encarguen únicamente de tratar los casos de vigilancia en un solo camino, pues desde la ciudadanía y diferentes organismos se promueven también mecanismos de contrainteligencia o, por ponerlo en términos más comunes, de defensa y protección de los datos y las comunicaciones que se desean privadas.

130 El Espectador. 10 de marzo de 2015.
131 El Espectador. 22 de julio de 2015.
132 El Espectador. 20 de mayo de 2015.
133 El Espectador. 29 de agosto de 2015.

Para hablar de encriptación es necesario enmarcarlo en un concepto más amplio y preciso que es la criptología (cryptology por su denominación en inglés). Según Dumas & Roch (2015), la criptología es entendida como la "ciencia del secreto" y está compuesta de la criptografía y el criptoanálisis (conocido también como *hacking*): la primera, pretende estudiar y construir los procesos de encriptación de la información, y el segundo analizar los textos cifrados con la finalidad de recuperar la información escondida.

La criptografía tiene como finalidad la confidencialidad e integridad de la información o comunicación pretendida, así como la autenticación de acceso por parte de los protagonistas o agentes emisores y receptores de dicha información o comunicación (Dumas & Roch, 2015).

Vale la pena añadir a este apartado conceptual que la encriptación es entonces vista como una tecnología que posibilita la privacidad, especialmente después de lo mostrado por Snowden, afirma Rider (2016), en tanto juega un papel muy importante para asegurar los derechos en Internet.

En este contexto, se resaltan los siguientes recortes en los que la encriptación es mencionada:

> *"... el Consejo de DD.HH. de la ONU aprobó recientemente un informe sobre anonimato y encriptación como parte del derecho a la libertad de expresión, el derecho a participar del ambiente online de modo anónimo para proteger el ejercicio de este derecho, y también el derecho que tienen las personas a protegerse de la invasión de estas tecnologías con mecanismos como la encriptación y otros que deberían popularizarse y estar al alcance de la gente, y la necesidad de educar en el uso de la seguridad y protección en internet"*[134].
>
> *"La Relatoría para la Libertad de Expresión explica que el software de espionaje comercializado por HT "estaría diseñado para evadir la encriptación en los computadores y teléfonos móviles, lo que permitiría sustraer datos, mensajes, llamadas y correos, conversaciones de voz a través de IP (VOIP, voice over IP) y mensajería instantánea"*[135].

[134] El Espectador. 26 de julio de 2015.
[135] El Espectador. 22 de julio de 2015.

*"A veces la actividad de los "hacker" resulta muy controvertida… hacker se denomina a quienes consiguen directamente la información en internet. No al que la compra o la vende"*[136].

*"¿La actividad del "hackeo" siempre es criminal e ilícita? No. Las empresas contratan hacker profesionales que hacen un trabajo legal y necesario para que encuentren sus vulnerabilidades mediante ataques controlados o intentos de sustracción de su información y las ayuden a blindarse de esas debilidades"*[137].

*"El argumento de fondo en esta discusión dice algo así: en la medida que la encriptación impide el acceso de los Estados a las comunicaciones, estas tecnologías se convierten en el canal preferido para los terroristas. La hipótesis es casi tan vieja como el terror mismo"*[138].

*"Lo cierto es que la comunicación encriptada y anónima no sólo es usada por terroristas, pues al ser una herramienta de acceso público también es una de las mejores aliadas de disidentes políticos y activistas de derechos humanos"*[139].

*"El cifrado es como un cuchillo: la herramienta en sí misma no es letal, depende del uso que se le dé"*[140].

*"Saber cómo se pueden proteger las comunicaciones personales y qué mecanismos existen para hacerlo, y que los estados promuevan esos mecanismos, traería un cambio sustantivo"*[141].

A pesar de que la encriptación resulta como un mecanismo fundamental que mantiene la privacidad en alto, no es suficiente para evitar totalmente el acceso a la información producida en medios digitales. Así lo hace ver el siguiente recorte:

*"El punto es que, incluso sin acceso a la encriptación, las autoridades pueden obtener datos sensibles sobre las comunicaciones mediante el rastreo de los metadatos: aunque no puede conocerse el contenido exacto de una llamada o un mensaje de texto, sí se puede saber quién está hablando con quién e incluso desde qué lugares; esta información puede ser suficiente para prevenir atentados, insisten expertos en seguridad informática"*[142].

## 6.7. Fuerza pública y vigilancia estatal masiva

En relación a la sección de inteligencia, las fuerzas armadas del Estado resultan ser organismos fundamentales en el ciclo de adquisición y gestión de los sistemas de

136 El Espectador. 25 de julio de 2015.
137 El Espectador. 25 de julio de 2015.
138 El Espectador. 18 de noviembre de 2015.
139 El Espectador. 18 de noviembre de 2015.
140 El Espectador. 19 de noviembre de 2015.
141 El Espectador. 26 de julio de 2015.
142 El Espectador. 18 de noviembre de 2015.

vigilancia masiva por parte de los Estados. Por esta razón, es la categoría más mencionada en las noticias del corpus del presente trabajo:

> *"¿Cuáles agencias usan sistemas de vigilancia masiva en Colombia? Las que mencionamos en el reporte: la Policía y dos de sus dos ramas, Dijín y Dipol"*[143].

> *"El año pasado, la ONU les envió varias comunicaciones tanto a Hacking Team como al representante de Italia ante las Naciones Unidas preguntando por qué Hacking Team le había vendido el software RCS a Sudán, país que tenía un embargo de armas y que podía usar ese programa "para inteligencia militar electrónica"*[144].

> *"... expone cómo las agencias de inteligencia de la Policía están desarrollando estos sistemas sin vigilancia pública ni bases jurídicas suficientes"*[145].

> *"¿En qué está usando la Policía el software de Hacking Team? En la detección de amenazas de la criminalidad organizada. La herramienta está enfocada en orientar a los grupos investigativos que combaten delitos como la extorsión"*[146].

Llama la atención la militarización que se le da a los medios de comunicación como intermediarios de vigilancia e inteligencia; el mismo Lash (2007) afirmaba que los medios de comunicación serían funcionales a los dispositivos de dominación. Al respecto se puede identificar el siguiente recorte:

> *"Pero quizás uno de los mayores riesgos para la red es su creciente transformación de medio de comunicación a campo de batalla para militares y gobiernos de todo el planeta"*[147].

## 6.8. Seguridad y vigilancia estatal

La seguridad es la primer movilizante y la primer causal para la implementación de sistemas de vigilancia (Bauman & Lyon, 2013), y así lo hacen ver varios recortes:

> *"... en el mundo del terrorismo la vigilancia masiva contra ciudadanos comunes y corrientes no sólo es conveniente, sino necesaria"*[148]*[Entrevista].*

> *"La seguridad nacional y la privacidad no se excluyen mutuamente. Ambas pueden lograrse a través de la recolección responsable de inteligencia, que respete las libertades de los ciudadanos que siguen la ley"*[149].

---

143 El Espectador. 29 de agosto de 2015.
144 El Espectador.11 de julio de 2015.
145 El Espectador. 30 de agosto de 2015.
146 El Espectador. 20 de febrero de 2016.
147 El Espectador. 14 de abril de 2015.
148 El Espectador. 3 de junio de 2015.

*"Los cambios en Estados Unidos, así como el debate abierto en lugares como Paraguay, parecen señalar nuevos caminos para balancear la necesidad de seguridad y vigilancia en la era del terrorismo con las oportunidades y libertades que otorga la red para todos"*[150].

*"La respuesta de la entidad fue un comunicado en el que indicó que "el propósito de esta compra fue potencializar la capacidad de detección de amenazas del terrorismo y la criminalidad organizada en el ciberespacio. En un país como éste, que la Fuerza Pública recurra a todas las herramientas posibles para combatir el crimen es lo mínimo que los ciudadanos esperan"*[151].

*"es clara la intencionalidad del gobierno de espiar a los ciudadanos. No se habla de contrataciones para combatir la delincuencia y la criminalidad, sino de espías a ciudadanos"*[152].

*"... el pulso entre el acceso a la información y la seguridad, entre la privacidad y las labores de inteligencia en un planeta aterrorizado, es una de las tensiones más importantes y necesarias a la hora de definir cómo será el crecimiento futuro de internet y con éste el de aquellos que hoy usan y usarán la red"*[153].

*"... que cuando estas tecnologías se utilicen para fines legítimos, como la seguridad, la lucha contra el terrorismo o el crimen organizado, estén claramente definidos los tiempos en los cuales se van a utilizar"*[154].

La implementación de sistemas de vigilancia masiva como los mencionados a lo largo del presente trabajo, conlleva a resultados que afectan la concepción misma de seguridad como lo muestran los siguientes recortes:

*"Debilitar la seguridad de todos en Internet no es la panacea que nos van a vender. Lo que sí hará de seguro es afectar la seguridad de todos"*[155].

*"... el problema de usar internet como un vehículo de combate es su potencial para fracturar la globalidad y apertura de este medio de comunicación mediante lo que se conoce como balcanización de la red: la creación de redes locales que, bajo la premisa de ser más seguras, aíslan ciertas porciones del tráfico en línea del resto de las conexiones mundiales, algo así como parcelar internet".*

Así es válido apuntar que más allá de la misma afectar la misma privacidad, este tipo de vigilancia influye en otros efectos secundarios, de no menor importancia y que son pasados por alto al momento de su contratación e implementación:

---

149 El Espectador. 3 de junio de 2015.
150 El Espectador. 3 de junio de 2015.
151 El Espectador. 11 de julio de 2015.
152 El Espectador. 22 de julio de 2015.
153 El Espectador. 20 de mayo de 2015.
154 El Espectador. 26 de julio de 2015.
155 El Espectador. 19 de noviembre de 2015.

*"El Estado debe poder usar las herramientas a su alcance para protegerse y protegernos, pero no analizar los riesgos y retos de hacerlo con perspectiva de derechos humanos es un error"[156].*

## 6.9. Casos de vigilancia estatal en Colombia y el mundo

A modo de conteo únicamente, se hizo el ejercicio de citar a continuación aquellos recortes en los que se demuestra la amplia cobertura en los medios de los diferentes casos de vigilancia estatal en Colombia y en el extranjero. Esto es importante en la medida que la vigilancia estatal ha estado en constante movimiento, demostrado anteriormente por el énfasis en las contrataciones de estas tecnologías y que, por tanto, no se han quedado por fuera de los medios de comunicación, en este caso la prensa. Se muestran a continuación los recortes:

*"… Edward Snowden, extécnico de la CIA, quien filtró documentos en los que mostraba cómo la Agencia Nacional de Seguridad de Estados Unidos (NSA, por sus siglas en inglés) estableció una red de vigilancia sobre las comunicaciones de millones de ciudadanos, una operación que realizó en conjunto con agencias de inteligencia de países como el Reino Unido"[157].*

*"De acuerdo con un detallado reporte del Citizen Lab, de la Universidad de Toronto, "Gran Cañón" permite realizar una tarea esencial que, a la vez, puede servir a dos propósitos. La herramienta logra manipular el tráfico en línea para redirigirlo hacia un blanco determinado y, de esta forma, utilizar ese flujo de datos (conexiones de usuarios que no saben qué sucede) como munición para tumbar un sitio web determinado"[158].*

*"Documentos publicados por WikiLeaks revelaron que los servicios de inteligencia y seguridad australianas negociaron de manera secreta con la empresa de ciberespionaje Hacking Team"[159].*

*"Las supuestas negociaciones entre la empresa y los servicios australianos giraban en torno al programa de vigilancia y espionaje Sistema de Control Remoto (RCS, siglas en inglés)"[160].*

*"La tecnología se llama Da Vinci y, por supuesto, es una de la formas más invasivas de hacer espionaje. Según la información revelada, el Gobierno colombiano, a través de la Dirección de Inteligencia de la Policía Nacional, parece ser uno de los compradores estrella, ya que aparecen pagos atribuidos a Puma, la plataforma de vigilancia de las comunicaciones que ya había sido cuestionada en el 2013"[161].*

156 El Espectador. 18 de agosto de 2016.
157 El Espectador. 10 de marzo de 2015.
158 El Espectador. 14 de abril de 2015.
159 El Espectador. 9 de julio de 2015.
160 El Espectador. 9 de julio de 2015.
161 El Espectador. 10 de julio de 2015.

*"Estas aseveraciones se prestaron para un sainete en el que el fiscal Montealegre evidenció la incompatibilidad con la plataforma para interceptaciones Esperanza y dijo con buen tino que Puma se prestaba para abusos, que no era necesaria y que aumentaba la intranquilidad de las personas"*[162].

*"No basta con todo el historial de chuzadas del DAS, ni los escándalos de háckers y andrómedas sino que los organismos de inteligencia ahora adquieren software malicioso y aumentan el riesgo de violaciones y abusos"*[163].

*"Para empezar, la Policía señaló que "no ha sostenido vínculo comercial con la firma Hacking Team", sino con Robotec Colombia S. A., lo cual podría ser una verdad a medias. Por una parte, según le explicó el gerente de Robotec, Jaime Caicedo, a este diario, lo que la Policía adquirió fue la licencia de un software cuya propiedad y derechos le pertenecen al fabricante, que es Hacking Team (HT). El Espectador le preguntó a Caicedo si la Policía sabía que HT estaba detrás del negocio, pero la respuesta de Caicedo se limitó a explicar a quién le pertenecía el software"*[164].

*"Si Robotec era el aliado de HT y Nice, ¿por qué se habla del negocio Puma (Plataforma Única de Monitoreo y Análisis) como algo aparte? ¿Le ofrecieron dos veces lo mismo a la Policía, como decían otros mensajes, o eran negocios distintos?"*[165].

*"Todo esto es lo que ofrece el programa de espionaje que la empresa italiana Hacking Team (HT) bautizó en honor a dos de sus más prominentes compatriotas: "Galileo" y "Da Vinci". El mismo software que le presentaron a la Fiscalía el año pasado. Ése que la Policía adquirió en 2013. El que en 2008 le ofrecieron nada más y nada menos que al DAS"*[166].

*"Galileo es un CNE (computer network exploitation) que Hacking Team personaliza a petición del cliente (agencia de inteligencia) con base en el perfil del objetivo"*[167].

*"Esperanza", en cambio, está descrito como una plataforma que requiere que la Fiscalía contacte a un proveedor de comunicaciones para pedir información sobre un blanco específico: es un proceso activo de interceptación. Puma y el sistema de la Dipol son pasivos y están diseñados para la recolección y análisis de datos a gran escala"*[168].

*"Entre el 29 de noviembre y el 2 de diciembre de este año la periodista Vicky Dávila recibió 170 correos de alguien que se presenta como "un policía arrepentido". En ellos se habla de seguimientos ilegales en contra de la comunicadora y otros periodistas. Y, lo que es peor, se adjuntan documentos reservados, como prueba de los seguimientos"*[169].

*"El síndrome de las chuzadas sigue intacto y algunos oficiales en la Policía, no se sabe por qué órdenes, lo siguen haciendo"*[170].

---

162 El Espectador. 10 de julio de 2015.
163 El Espectador. 10 de julio de 2015.
164 El Espectador. 11 de julio de 2015.
165 El Espectador. 11 de julio de 2015.
166 El Espectador. 18 de julio de 2015.
167 El Espectador. 23 de julio de 2015.
168 El Espectador. 29 de agosto de 2015.
169 El Espectador. 4 de diciembre de 2015.
170 El Espectador. 12 de diciembre de 2015.

*"La plataforma, conocida como Pegasus, permite cosas como extracción de mensajes de texto, listas de contacto, citas de calendario, correos electrónicos y ubicaciones de GPS. Además, puede activar secretamente el micrófono de un teléfono, así como la cámara. Todos estos datos pueden ser transmitidos en tiempo real a los servidores de quien realiza la interceptación"*[171].

*¿Usan la Policía y la Fiscalía el software Link Analysis o alguno similar? ¿Usan IMSI catcher o malware para control remoto? Si es así, podrían informarnos ¿cómo y con qué fines se adquirió, quién lo utiliza y bajo qué protocolos y supervisión?* [172]

## 6.10. TIC's y vigilancia estatal masiva

La conversación mantenida respecto a la relación entre tecnologías de información y vigilancia estatal radica principalmente en los alcances que estas posibilitan para la obtención de mayor cantidad de datos y las facilidades para su posterior gestión (Mayer-Shonberger & Cuckier, 2013; Fuchs; 2014). En este apartado se destacan los siguientes recortes:

*"La dinámica no es nueva, pues en últimas una guerra es, al menos en parte, el aprovechamiento de una tecnología para superar a un rival, desde la pólvora, pasando por el gas mostaza, el fósforo blanco y el poder del átomo hasta la manipulación del universo digital del enemigo, así éste sean los usuarios civiles de ese universo"*[173]**.**

*"En la cableada es muy difícil [interceptar] porque se necesita la presencia física, en la central telefónica, de quien esté haciendo el monitoreo; en la inalámbrica hay que capturar la señal en el espectro, es decir, en el aire. Y en la digital se puede interceptar de manera sencilla, tal cual se hace como cuando se monitorea un celular"*[174].

*"... es que los sistemas y tecnología deben siempre estar adaptándose a los cambios en las amenazas"*[175].

*"Colombia, como cualquier otro país, necesita herramientas para combatir la criminalidad. Pero el software de espionaje que escogió para hacerlo, el RCS de Hacking Team, ha sido duramente cuestionado desde antes de que Colombia lo adquiriera"*[176].

*"Hoy hay software disponible y aplicaciones que ya incluyen la posibilidad de proteger las comunicaciones que tenemos"*[177].

---

171 El Espectador. 5 de septiembre de 2016.
172 El Espectador. 10 de septiembre de 2015.
173 El Espectador. 14 de abril de 2015.
174 El Espectador. 25 de julio de 2015.
175 El Espectador. 20 de mayo de 2015.
176 El Espectador. 11 de julio de 2015.
177 El Espectador. 26 de julio de 2015.

> *"Es claro que el Distrito debe adquirir un mayor número de cámaras de seguridad, ya que son una herramienta tecnológica clave para las autoridades al momento de la identificación a los responsables de un delito"*[178].

> *"HT discutía una propuesta técnica con la Policía colombiana, en la que, según reza el documento publicado en Wikileaks, se le ofreció el paquete de herramientas para infectar Android (sistema operativo móvil de Google, presente en más del 70% de los teléfonos inteligentes a nivel mundial), iOS (dispositivos de Apple), así como computadores de escritorio con Windows o Mac OS X, entre otras plataformas. Las negociaciones incluían un precio especial de compra si ésta llegaba a realizarse antes del 30 de junio (850 mil euros)"*[179].

También llama la atención a la relación que existe entre la tecnología y la legislación en el marco de los sistemas de vigilancia, comprendiendo de antemano que la primera está en constante y acelerado cambio y la segunda no tiene las condiciones de seguir dicha dinámica (Cortés Castillo, 2014), a pesar de que el legislador es el más indicado para atender como ente de control los afanes y preocupaciones que la tecnología trae consigo. Al respecto, se han encontrado los siguientes recortes:

> *"Aunque el desarrollo de las tecnologías avanza más rápido que el derecho, existen principios para que estas herramientas no vulneren la libertad y dignidad de los ciudadanos"*[180].

> *"Si Colombia sigue estos consejos y desarrolla herramientas concretas de política pública para manejar las tensiones específicas que se presentan frente a la tecnología, la intimidad y otros derechos fundamentales, habrá comenzado a demostrar lo que todos esperamos: que la tecnología está para vigilar el poder y no lo contrario"*[181].

Existe una preocupación sobre el conocimiento de las realidades de la vigilancia estatal y masiva a partir de los medios de comunicación, algo que Andrejevic (2014) hace llamar como la brecha *big data* haciendo un llamado a la diferencia entre los conocimientos y alcances que los Estados tienen de los sistemas de vigilancia, sus causas, usos y consecuencias, y la ciudadanía del común que rara vez tiene siquiera un proceso de concientización. Esto lo hacen ver los siguientes recortes, haciendo una mención de la importancia de la educación en estos temas:

---

178 El Espectador. 14 de julio de 2016.
179 El Espectador. 22 de julio de 2015.
180 El Espectador. 22 de julio de 2015.
181 El Espectador. 11 de noviembre de 2016.

*"En el mundo actual, la educación para el uso de estas herramientas [de encriptación] es fundamental para poder ejercer y garantizar derechos"*[182].

*"... una vez la gente comienza a entender lo que se puede hacer con estas herramientas, empieza a cuestionar el propósito para el cual fueron diseñadas y no las leyes que las regulan"*[183].

## 6.11. Internet y vigilancia estatal masiva

Internet como medio de comunicación resulta fundamental para entrar en la discusión de la vigilancia estatal y masiva, en tanto es la fuente de información y medio de comunicación por donde transitan todos los datos que pueden y no pueden (a razón de la encriptación) ser rastreados, recolectados, almacenados, organizados y perfilados (Castells, 1999; Fuchs, 2014; Kerr & Barrigar, 2012; Parliament of United Kingdom, 2009; Wall, 2007). Al respecto se resaltan los siguientes recortes:

*"Me acuerdo de cuando la red era un lugar libre y de verdad servía para comunicar a la gente. Ahora todos esperan ser vigilados y se abstienen de expresar ciertas opiniones o afiliarse a un movimiento político determinado por miedo a ser espiados"*[184].

*"Para todas sus bondades, internet sigue siendo una herramienta que no termina de salir de una cierta adolescencia, un tiempo que, casi por definición, está plagado de complicaciones y obstáculos"*[185].

*"Pero quizás uno de los mayores riesgos para la red es su creciente transformación de medio de comunicación a campo de batalla para militares y gobiernos de todo el planeta"*[186].

*"Entre otros asuntos, el problema de usar internet como un vehículo de combate es su potencial para fracturar la globalidad y apertura de este medio de comunicación mediante lo que se conoce como balcanización de la red: la creación de redes locales que, bajo la premisa de ser más seguras, aíslan ciertas porciones del tráfico en línea del resto de las conexiones mundiales, algo así como parcelar internet"*[187].

*"... el pulso entre el acceso a la información y la seguridad, entre la privacidad y las labores de inteligencia en un planeta aterrorizado, es una de las tensiones más importantes y necesarias*

182 El Espectador. 26 de julio de 2015.
183 El Espectador. 29 de agosto de 2015.
184 El Espectador. 4 de febrero de 2015.
185 El Espectador. 17 de mayo de 2016.
186 El Espectador. 14 de abril de 2015.
187 El Espectador. 14 de abril de 2015.

*a la hora de definir cómo será el crecimiento futuro de internet y con éste el de aquellos que hoy usan y usarán la red"*[188]*.*

Se destacan las posiciones críticas de los anteriores recortes pues se mencionan efectos secundarios de un Internet vigilado como la "balcanización de la red", la militarización de los medios de comunicación, y el análisis más a fondo de lo que se esperaría de Internet cada vez más dispuesto y construido en función de propósitos de control y dominación.

## 6.12. Plataformas de redes sociales, vigilancia y privacidad de información

La vigilancia en las redes sociales hace parte del mundo de vigilancia planteado por Bauman & Lyon (2013); por ende, la privacidad no se espera o es indefinida en las redes sociales, esto lo hicieron saber Dwyer, Hiltz & Passerini (2007) comprendiendo que la información allí contenida era parte de un proceso de minería de datos para posterior comercialización con fines publicitarios. Al respecto se pueden resaltar los siguientes recortes:

*"El director de Facebook para el Cono Sur, Alejandro Zuzenberg, dijo este viernes que la red social, que ya suma más de 1.400 millones de usuarios, no vende bases de datos y que no existen herramientas para hacerlo"*[189]*.*

*"Según el líder para el Cono Sur, la publicidad que aparece en Facebook, muchas veces cuestionada en relación a la privacidad de las personas, es solo una herramienta para que una empresa o página promueva historias que publica y en el momento de hacerlo tiene opciones para elegir qué personas la pueden ver"*[190]*.*

*"A pesar de la cantidad de adherentes, la red social fundada por Mark Zuckerberg se enfrenta a una demanda colectiva que agrupa a más de 75 mil usuarios, que acusan a Facebook de utilizar ilegalmente sus datos personales"*[191]*.*

De otra manera, otras redes sociales y empresas de tecnologías se han visto comprometidas en el sentido de que los Estados han solicitado disponer de puertas

188 El Espectador. 20 de mayo de 2015.
189 El Espectador. 24 de abril de 2015.
190 El Espectador. 24 de abril de 2015.
191 El Espectador. 24 de abril de 2015.

traseras en las comunicaciones encriptadas para tener acceso a s los contenidos que transitan por sus servidores. Esto lo hace ver el siguiente recorte:

> *"Los mayores hallazgos del informe se pueden resumir de esta forma. Del grupo analizado, sólo nueve empresas cumplen completamente con los criterios esbozados por la EFF: Adobe, Apple, CREDO, Dropbox, Sonic, Wickr, Wikimedia, Wordpress y Yahoo. AT&T, Verizon, y WhatsApp recibieron las calificaciones más bajas. "Una mayoría abrumadora de compañías de tecnología se opone a las puertas traseras ordenadas por el gobierno", añade en un tercer punto el documento"*[192].

> *"Escuchar y hasta grabar llamadas de Skype. Acceder a emails y a aplicaciones de chat como Whatsapp, Viber, Hangout o Telegram"*[193].

En enero de 2016 Facebook lanzó una campaña titulada *"Initiative for Civil Courage Online"* que pretendía a partir de un desarrollo tecnológico en particular evitar la publicación y viralización de contenidos con discursos de odio o con contenidos amenazantes (Griffin, 2016). En relación a esta temática se han puesto en cuestión los parámetros de dicha campaña y se ha problematizado porque tendría la tendencia por afectar expresiones de disenso; al respecto se relaciona el siguiente recorte:

> *"El primero tiene que ver con la responsabilidad de Facebook ante la justicia de países diferentes a Estados Unidos (Francia, en este caso) y el segundo está relacionado con la forma como servicios en línea pueden afectar la libertad de expresión e incluso el derecho de asociación mediante la aplicación de políticas que, buscando repeler la pornografía, afectan expresiones humanas como el arte o el disenso; en últimas, se trata de cómo una compañía privada puede terminar imponiendo un modelo moral de aproximarse al mundo, una empresa dirigida por alguien de 31 años"*[194].

Sin embargo, también se encuentra entre las noticias algunas buenas prácticas de las redes sociales para proteger la privacidad de los usuarios o por lo menos, muestran una mayor cantidad de información respecto al manejo y control de datos personales. Se hace saber en los siguientes recortes:

---

192 El Espectador. 18 de junio de 2015.
193 El Espectador. 18 de julio de 2015.
194 El Espectador. 8 de marzo de 2015.

*"Esos controles, entonces, quizá podrían provenir de las buenas prácticas de las empresas, como la publicación de informes de transparencia, un asunto que se ha vuelto bastante común entre compañías de tecnología como Google, Twitter o Facebook, por mencionar algunas"*[195].

*"Facebook anunció este viernes que ofrecerá una opción de "encriptación de punta a punta" para los usuarios de su aplicación Messenger, siguiendo una tendencia que apunta hacia una mejor seguridad y protección contra la vigilancia electrónica… Uno de los puntos débiles de la iniciativa es que, a diferencia del cifrado que ofrece WhatsApp, esta herramienta no funciona por defecto, sino que debe ser encendida por cada usuario"*[196].

[195] El Espectador. 20 de mayo de 2015.
[196] El Espectador. 8 de julio de 2016.

# CAPÍTULO VII. PRENSA DIGITAL Y DERECHO A LA PRIVACIDAD DE INFORMACIÓN

Los resultados respecto de la privacidad de la información se relacionan con el concepto principal del derecho a la privacidad desde un marco de derechos humanos que se aborda desde la legalidad propia de cada Estado. De igual manera, se habla del rompimiento de los límites de la privacidad de la información y la cualidad económica que pueden contar en la actualidad, en relación directa con la protección de datos.

También se hace evidente una mención de los efectos de las TIC's en la privacidad de información, destacando principalmente sus peligros para el ejercicio de desarrollo personal como para el desarrollo ciudadano-político.

## 7.1. Derecho a la privacidad y derechos humanos asociados

Hay una preocupación constante de la privacidad como un derecho humano. A pesar de esto, parece que la vigilancia en razón de la seguridad tiene mayor relevancia para los Estados según los hechos reportados; aun así, esta preocupación de la ciudadanía se ve afectada por un desconocimiento de fondo acerca de la importancia de la privacidad y del alcance mismo que la vigilancia estatal está alcanzando. Es así que se cuestiona constantemente cómo se legaliza respecto a la privacidad, que al ser una construcción social (Solove, 2010), se puede construir una sociedad más democrática y en defensa de las libertades que demanda.

> *"La seguridad nacional y la privacidad no se excluyen mutuamente. Ambas pueden lograrse a través de la recolección responsable de inteligencia, que respete las libertades de los ciudadanos que siguen la ley"*[197].

[197] El Espectador. 3 de junio de 2015.

*"Los expertos sostienen que el cambio sustancial actual es que la gente se ha dado cuenta del peligro que corre su intimidad y su privacidad … La información personal que antes se consideraba intocable, por ejemplo, números de cuentas bancarias, estados financieros personales, direcciones y teléfonos no publicados, dejó de tener garantizada su privacidad ¿Estamos inermes, legalmente hablando, en el país ante esta realidad? No. Hay garantías de privacidad"*[198].

*"El conocimiento del público sobre estos temas es muy bajo. Esto no es conveniente en un escenario en el cual las agencias de inteligencia o de la Policía pueden estar tomando acciones contra un derecho fundamental: la privacidad"*[199].

*"... es fundamental que el Senado estudie los contratos, documentos y políticas que existen en relación con este tipo de sistemas de vigilancia para que, de esta manera, entienda el alcance de este problema y pueda hacer las auditorías necesarias para evitar cualquier violación al derecho a la privacidad"*[200].

*"La protección efectiva del derecho a la privacidad debe provenir en parte de la creación de mejores leyes para evitar que las agencias de la Policía tengan la capacidad de interceptar información de manera masiva"*[201].

*"¿O creemos que hay mucho riesgo de abuso en la vasta cantidad de información privada que producen estas actividades, y que en estos riesgos no sólo se juega la privacidad de los ciudadanos, sino los derechos humanos y la democracia, como para permitir que este sistema siga operando?"*[202].

*"... los derechos humanos requieren que cualquier interferencia a la privacidad sea legítima, necesaria en un entorno democrático y proporcional"*[203].

*"... dentro de los principios que establece el Conpes se encuentra "salvaguardar los derechos humanos y los valores fundamentales de los individuos, incluyendo la libertad de expresión, el libre flujo de información, la confidencialidad de la información y las comunicaciones, la protección de los datos personales y la privacidad…* [204]

*"... políticas vagas y poco claras, además de ausencia de transparencia acerca del rol que cumplen estas empresas en la entrega de información personal al Gobierno, dejan mucho espacio para mejorar"*[205].

Siendo así, el tema tecnológico parece marcar una diferencia en el marco legal de la privacidad como derecho, algo que no es desconocido para Fornaciari (2014), quien afirma que desde este marco la ley no parece responder a las demandas que

198 El Espectador. 25 de julio de 2015.
199 El Espectador: 29 de agosto de 2015.
200 El Espectador. 30 de agosto de 2015.
201 El Espectador. 30 de agosto de 2015.
202 El Espectador. 6 de octubre de 2015.
203 El Espectador. 5 de septiembre de 2016.
204 El Espectador. 4 de febrero de 2016.
205 El Espectador. 20 de mayo de 2015.

desde las tecnologías hacen las instituciones sociales y la ciudadanía. A la prensa no le es ajeno este marco legal, tecnológico y social, por lo que hay un esfuerzo por abarcar a la privacidad de manera contextual, siendo un llamado constante por los expertos de esta materia (Noaín Sánchez, 2015; Fornaciari, 2014; Nissembaum, 2010).

> *"... el escándalo de interceptaciones estadounidenses motivó la adopción (promovida por Brasil y Alemania) de una resolución de la Asamblea General de la ONU sobre "el derecho a la privacidad en la era digital", que menciona "una preocupación por la posible afectación del ejercicio y goce de DD.HH. por actos de vigilancia e interceptación de comunicaciones masivas o extraterritoriales, donde se exhorta a que los Estados actúen de forma respetuosa de aquellos derechos en el ámbito de internet"[206].*
>
> *"Ahora, si bien las nuevas tecnologías están avanzando nuestras libertades, también están permitiendo la invasión de nuestra privacidad sin precedentes"[207].*
>
> *"Nos parece de la mayor preocupación porque este tipo de tecnología está diseñada para la intromisión en la privacidad a través de mecanismos digitales que permiten recolectar datos sin el conocimiento de las personas o instalar programas sin autorización en los dispositivos"[208].*
>
> *"no es claro el alcance de lo que se les ordena retener a los proveedores de redes y servicios de comunicaciones"[209].*
>
> *"la normativa de inteligencia no contempla la notificación a los usuarios de la realización de actividades de vigilancia de las comunicaciones en su contra (...). En otras palabras, en Colombia una persona no puede consultar si existen o han existido en el pasado acciones de inteligencia en su contra, ni pedir su corrección, ni hay un juez que controle la realización de ciertas actividades de inteligencia que inciden en sus derechos fundamentales"[210].*
>
> *"... los agentes pueden acceder indiscriminadamente a la información del dispositivo e instalarle programas y archivos, también pueden recopilar, retener y usar incontables datos personales"[211].*
>
> *"En esa lógica imagine que los gobiernos pasen de ordenar a las empresas crear puertas traseras en sus productos y decidan que deben incluirlas también en el diseño de los grandes servicios de información personal de la ciudadanía"[212].*

---

206 El Espectador. 22 de julio de 2015.
207 El Espectador. 17 de mayo de 2016.
208 El espectador. 26 de julio de 2015.
209 El Espectador. 20 de mayo de 2015.
210 El Espectador. 20 de mayo de 2015.
211 El Espectador. 23 de julio de 2015.
212 El Espectador. 25 de febrero de 2016.

También ha sido común encontrar derechos relacionados a los de privacidad y que se han visto afectados por la vigilancia estatal, como lo son la libertad de opinión y expresión, y la libertad de agrupación y asociación, las cuales han sido asunto continuo de mención y preocupación de varias organizaciones sin ánimo de lucro y la Organización de las Naciones Unidas (2014)".

> *"... la iniciativa [de vigilancia estatal en Paraguay] "daña derechos constitucionales como la privacidad, asociación y libertad de expresión, porque lo que propone esta ley es la vigilancia masiva de las personas, como si todas fueran culpables"[213].*
>
> *"Cuando esto se hace sin un marco jurídico adecuado, sin control judicial, sin claridad en los objetivos o intereses que persigue el Estado, supone una vulneración del derecho a la privacidad y del derecho a la libertad de expresión, en el sentido de que para ejercer este derecho, que incluye la construcción de pensamiento, la búsqueda de información y el desarrollo de investigaciones, las personas necesitan garantías de no ser espiadas ni vigiladas"[214].*

## 7.2. Privacidad y economía de la información

Si bien los casos abordados en el estudio son de carácter estatal, no quedan por fuera de la discusión los efectos de la economía de la información en la disrupción de la privacidad de las personas. Son constantes las discusiones respecto a los intereses económicos y políticos de la información privada de las personas; Fuchs (2011b) hace evidente esta realidad en su propuesta sobre un concepto alternativo de privacidad en el que los detalles económicos de las grandes empresas y Estados debe ser totalmente conocido por el mundo, y la información del 99%[215] de las personas del mundo sea protegida para su propio desarrollo en función de sus expectativas.

Teniendo en cuenta esta perspectiva, se encontraron recortes en relación a preocupaciones sobre el uso económico de datos personales que son dados, en la mayoría de casos, inconscientemente:

---

[213] El Espectador. 10 de marzo de 2015.
[214] El Espectador. 26 de julio de 2015.
[215] Entiéndase el 99% como la proporción de personas que no son parte del comparativamente pequeño grupo que tiene gran parte de la riqueza económica mundial y que adicionalmente tiene el poder de administrar y gestionar.

*"Según el líder para el Cono Sur, la publicidad que aparece en Facebook, muchas veces cuestionada en relación a la privacidad de las personas, es solo una herramienta para que una empresa o página promueva historias que publica y en el momento de hacerlo tiene opciones para elegir qué personas la pueden ver"*[216].

*"Estoy sorprendida, decepcionada y preocupada. Este proyecto de ley va más allá de la lucha contra el terrorismo porque incluye los intereses industriales, económicos y científicos de Francia. En nombre de todo ello se justifica la intrusión sistemática en la vida privada de las personas sin ningún control judicial"*[217].

## 7.3. Privacidad y protección de datos

Dentro de la conceptualización de privacidad de información planteada por Tavani (2008) se contempla la protección de datos entregados a las instituciones públicas y privadas, quienes tienen la obligación de salvaguardar su confidencialidad y asegurar su buen uso. Al respecto, se encuentran los siguientes recortes:

*"Dentro de los principios que establece el Conpes se encuentra "salvaguardar los derechos humanos y los valores fundamentales de los individuos, incluyendo la libertad de expresión, el libre flujo de información, la confidencialidad de la información y las comunicaciones, la protección de los datos personales y la privacidad (...)"*[218]

*"Los demandantes exigen que la compañía cese su vigilancia masiva, que tenga una política de protección de la vida privada comprensible y que deje de recabar datos de personas que no tienen cuentas con ellos"*[219].

*"Lo cierto es que, en cuanto a protección de datos de los usuarios, el peso no sólo recae en las empresas, que siempre son susceptibles de mejoras, sino también en el Estado, en las obligaciones que les impone a éstas"*[220].

*"Hay garantías de privacidad. En la Ley 1581 del 2012 Colombia adoptó todo un sistema de protección de datos personales y sensibles. Y ninguna entidad pública o privada puede darles trámite sin autorización libre, previa y expresa de su titular"*[221].

*"... el acceso de que disponen los servicios de información estadounidenses a los datos transferidos constituye una "injerencia" en la vida privada y viola la protección de datos personales, "concretamente porque la supervisión (...) es masiva e indiferenciada"*[222].

---

216 El Espectador. 24 de abril de 2015.
217 El Tiempo. 6 de mayo de 2015.
218 El Espectador. 4 de febrero de 2016.
219 El Espectador. 24 de abril de 2015.
220 El Espectador. 20 de mayo de 2015.
221 El Espectador. 25 de julio de 2015.
222 El Espectador. 23 de septiembre de 2015.

Se encuentra que a pesar de la obligación legal que tienen las empresas y los Estados de proteger los datos de las personas/ciudadanos, estos incurren en acciones que los trasgreden. Sin embargo, vale la pena destacar que se encuentran también buenas prácticas de empresas principalmente, que desarrollan estrategias de transparencia para ofrecer mejores servicios a sus clientes:

> *"Directv es consciente de la importancia de la seguridad de la información en el contexto actual, en donde la protección de la privacidad de las personas forma parte esencial de cualquier servicio. Directv cumple la normativa de protección de datos personales de todos sus usuarios de conformidad con las normas legales vigentes"*[223].

[223] El Espectador. 20 de mayo de 2015.

## CONCLUSIONES

Siendo la violencia uno de los principales problemas de la historia de la sociedad colombiana, durante 2015-2016 se mantuvieron las negociaciones y firma del proceso de paz entre las FARC y el Estado Colombiano, empezado en 2012. A pesar que los actores más visibles de la historia reciente en el país han sido las FARC, se destacan otros actores que han sido partícipes activos de este denominado conflicto armado interno, como los paramilitares, y la fuerza pública misma como representante del Estado. Como elemento adicional a esta realidad, el narcotráfico ha hecho parte desde los años 80's siendo un mercado ilegal con altibajos pero que ha permanecido en el imaginario de la ciudadanía y en las discusiones de política pública en Colombia.

En respuesta a este contexto socio-político, el país parece no responder directamente a su solución desde la implementación de tecnologías de vigilancia y la inevitable invasión a la privacidad de información de la ciudadanía, sino, a partir de la vencida justificación de la seguridad, usarlas con fines políticos. Además de que sí se hace visible una normativa respecto a la interceptación de comunicaciones y de protección de datos, en muchos casos se duda de su respectiva aplicación y alcances, pues en varios casos se denuncia que están pensadas para las instituciones privadas y públicas, pero no para la ciudadanía, siendo por tanto preocupante en un entorno en que la privacidad de información parece estar cada vez más transgredida.

Las instancias públicas mandadas a legislar y ejercer control sobre los sistemas de vigilancia y la interceptación de comunicaciones, como la Corte Constitucional y la Procuraduría, no realizan su trabajo en beneficio de la ciudadanía y sus derechos humanos. A diferencia, la Fiscalía, en el caso particular de PUMA (según varias acepciones, este sistema era el comercializado como Galileo o Da Vinci de Hacking Team y adquirido por la Policía Nacional), salió adelante a declarar que la única

entidad con la habilidad legal de hacerlo es la Fiscalía misma, denunciando además que los alcances de esta tecnología traspasaban las necesidades que pretendía atender.

La ciudadanía es la principal afectada en el contexto colombiano implementando tecnologías de vigilancia estatal masiva y selectiva, y se plantean algunas respuestas que desde el ejercicio ciudadano se pueden establecer como medios de defensa, enmarcados principalmente desde la encriptación de las comunicaciones, lo que en otras palabras sería esconder de la visión con la que cuentan las tecnologías de vigilancia aquellos mensajes que resulten importantes para su(s) emisor(es) y receptor(es). La barrera que se presenta acá es la brecha digital que separa los conocimientos informáticos que la encriptación requiere respecto a las capacidades y asesoría con la que cuentan los Estados para la implementación de tecnologías de interceptación, en comparación con los conocimientos de la ciudadanía en general.

El proceso de paz hizo parte de los procesos de vigilancia estatal en Colombia, en dos sentidos: uno, se reveló que varios periodistas que hacían seguimiento al proceso de paz en La Habana, fueron objetivos de vigilancia selectiva desde el Estado; y dos, en el desarrollo de política pública se realizaron sugerencias en función de que los procesos de inteligencia estuvieran pensados en un país en posconflicto, lo que llama la atención para futuras investigaciones interesadas en la conexión de la vigilancia con los procesos de posconflicto.

En el contexto colombiano se resalta entonces una pregunta o relación entre las categorías de justicia y vigilancia, entendiendo que el proceso de paz y su resultado de posconflicto demanda la comprensión entre unos procesos y objetivos de vigilancia que nunca se detendrán y de cómo se pueden legislar y configurar unos sistemas en función de cumplir con un proceso de justicia transicional de un país en camino social y político hacia la paz. Esta gran cuestión, que ha sido mencionada en

algunos recortes, no se encuentra profundizada, y se encuentra que puede plantear un amplio e interesante debate para la limitación de una vigilancia construida para los derechos humanos, la justicia y la paz.

Se encontró una relación entre democracia y vigilancia estatal, principalmente en relación a la afectación de una esfera pública con libertad de expresión en la que se imposibilita que la ciudadanía pueda ejercer control sobre sus discursos en una situación en la que sabe que está siendo observado con fines políticos, principalmente. Esto ha sido evidente en la historia del país (con las conocidas interceptaciones ilegales conocidas como 'chuzadas') y por tanto es un tema común pero necesario de abordar en los estudios de vigilancia y comunicación.

De la prensa escrita digital elegida, los medios de El Tiempo y El Espectador, se evidencia que el primero no cuenta con una agenda respecto a los temas de vigilancia estatal y privacidad de la ciudadanía, más allá de unas menciones o recortes al respecto; a diferencia, El Espectador cuenta con un fundamento y esfuerzo por dejar aunque sea un historial de lo ocurrido con los escándalos de los sistemas de vigilancia estatal en Colombia y el mundo, demarcando los efectos a los que se someten tanto los Estados como la ciudadanía en materia de derechos humanos, lo que viene a ser la categoría central de esta discusión, pasando también por un segundo nivel la problemática de la contratación pública como un aspecto de transparencia desde las instituciones de la fuerza pública como la policía y los servicios de inteligencia.

Respecto a la cobertura de los temas de vigilancia estatal y privacidad de la ciudadanía, se encontró que El Espectador sí realizó un seguimiento a los casos de Hacking Team y vigilancia estatal en Colombia, en función de los informes que fueron publicados al respecto por Privacy International (Gran Bretaña), Derechos Digitales (Chile) y Fundación Karisma (Colombia). A diferencia de esto, se encontró que la cobertura de El Tiempo no fue comparable y se tomaron sólo algunos

recortes de noticias aisladas respecto a los temas de interés. Los temas de mayor cobertura y relevancia fueron los relacionados a las adquisiciones de tecnologías de vigilancia por parte de la Policía Nacional a la empresa Hacking Team, a través de su distribuidor en Colombia, Robotec S.A; de igual manera, las agencias de inteligencia de todo el mundo salieron a relucir con gran hincapié dentro de las noticias, demostrando que son las encargadas de hacer uso de las tecnologías de vigilancia estatal, que en sus inicios estaban dadas para atender asuntos frente a amenazas extranjeras, pero que poco a poco se ha encargado de atender procesos también al interior de los países, y Colombia no ha sido la excepción, a pesar que la policía ha sido el principal actor en los casos resaltados durante el periodo seleccionado.

La tecnología también juega un papel fundamental en la discusión sobre los sistemas de vigilancia, entendiendo sus alcances técnicos en donde se pone en discusión la habilidad y conocimientos mismos de las instituciones del Estado colombiano en su completo y correcto uso. Es fundamental la presencia de la tecnología como una categoría de análisis en los estudios sobre vigilancia, con la finalidad de comprender su configuración, detalles particulares y ventajas en los contextos en los que se implementa.

Internet como medio, pero también como categoría de análisis, resulta fundamental para comprender completamente lo que la tecnología en los ámbitos de la información y la comunicación ha desarrollado. Para el caso de la vigilancia estatal y la fragilidad de la privacidad, toda la información binaria que se transporta a través de Internet pasa a ser cosechada, guardada, organizada y analizada, por lo que permite comprender la magnitud de la situación y la gravedad de dejar en manos de unos cuantos la información sobre lo que se comunica y lo que se hace. Esto pone en evidencia que la construcción de las tecnologías no es neutra, e Internet no se queda por fuera de esta premisa.

Se echa de menos una discusión sobre las posibilidades que tiene la ciudadanía de hacer contrainteligencia/contravigilancia al Estado, ya que el caso mismo de Hacking Team es la muestra de ello, en el que se pone en evidencia unas contrataciones de elementos dudosamente legales y legítimos, además de hacer uso de recursos públicos de manera poco transparente con el país. Esto se encuentra dentro de las posibilidades de la nueva vigilancia y permite ver que a pesar que sigue existiendo una brecha entre los Estados y la ciudadanía en Colombia, puede haber respuestas que generan un contrapeso a las malas prácticas que desde los ejercicios de poder se realizan.

Los casos de vigilancia estatal masiva y selectiva en Colombia y el mundo, permanecen a la sombra del conocimiento de la ciudadanía y, por tanto, el acercamiento que se le hace desde los medios se hace desde una posición de escándalo, secreto y transparencia. Los medios de comunicación en este aspecto, al asumir una agenda como lo hizo El Espectador, se convierten en los intermediarios entre la ciudadanía y aquellas organizaciones o sujetos que se han encargado de develar públicamente acciones dudosamente legales y con fines conocidos como ilegítimos. Existe, por tanto, una preocupación y denuncia constante, tomando como puntos de vista tanto al oficialismo como a expertos en materias de derechos humanos principalmente.

Los acercamientos desde los cuales se realizan denuncias a la vigilancia estatal es desde los derechos humanos que continuamente pone en duda, a saber, la privacidad, la libertad de expresión y la libertad de asociación, todas estas necesarias para el debate público y el desarrollo personal de cada persona. Es fundamental no dejar nunca a un lado de la discusión estos derechos humanos y los que estén asociados, ya que hacen parte de la columna central para debatir sobre la necesidad de una vigilancia masiva y selectiva desde los Estados, que como en algunos recortes se hacía saber, es posible hacer una vigilancia que responda a los

tres principios de la interceptación de comunicaciones: que sea necesaria, proporcional y legítima.

Cuando se habla de privacidad de la ciudadanía en los medios de comunicación, se encontró que su relevancia está dada principalmente por su condición de derecho humano y relación directa a otro como la libertad de expresión y asociación. En el contexto determinado, se encuentra que la protección de datos es un eje fundamental para la privacidad de la información, en tanto es la conceptualización usada comúnmente en la legislación, espacio en el que se ha hecho hincapié en Colombia desde las ONG exigiendo a las empresas de comunicaciones hacer un buen uso de la información y los datos que transfieren y guardan; al respecto, se encuentra una constante denuncia sobre que ni el Estado ni las empresas de telecomunicaciones hacen un buen uso de los datos de la ciudadanía en Colombia, a pesar de la legislación existente, pero que al hacer seguimiento, se empiezan a encontrar y destacar buenas prácticas en el uso de información ajena.

Llama la atención que dentro de la construcción de realidad respecto a los sistemas de vigilancia estatal haya menciones sobre los casos relacionados en el extranjero, en ambos medios, demostrando que es un tema relativamente nuevo para Colombia, donde se está acercando, construyendo y problematizando desde los medios y la academia.

A esta discusión resalta una pregunta acerca de si la vigilancia estatal masiva puede ser proporcional, necesaria y legítima. Los tres principios clave para una interceptación de comunicaciones se ven cuestionados cuando se habla de vigilancia masiva, por lo que las agencias de inteligencia estarán en constante cuestionamiento respecto a los alcances que pretenden lograr con estos sistemas, y bajo qué argumentos y circunstancias justificar atentar contra la privacidad de la ciudadanía en un contexto de democracia e igualdad.

Preocupa en la realización del presente trabajo de grado la fragilidad legal pero también académica en la cual se encuentra la privacidad en el mundo actual digitalizado. Más allá de comprender a la privacidad como un derecho humano, no se encuentran más condiciones que permitan fortalecerlo en discusiones donde la seguridad resulta como una necesidad para el desarrollo de cualquier sociedad; pareciera que la seguridad está muy por encima de la privacidad, sin embargo, ambas categorías pertenecen a ámbitos diferentes de desarrollo de la persona de no ser por la vigilancia cada vez más sensible que se ejerce desde los Estados y las diferentes instituciones sociales.

Un estudio sobre la agenda de los medios de comunicación como este, cumple con un múltiple propósito tanto para la academia como para el periodista o escritor que trabaja para estos. Por un lado, se pueden obtener en evidencia las temáticas tratadas y posteriormente, si se desea, profundizar en su tratamiento y acercamiento. Por otro lado, puede constituirse un suplemento adicional para encontrar nuevas categorías de estudio enmarcadas dentro de la categoría de interés de la investigación que las alcanzó. Por último, es claro que la investigación académica sirve como medio de denuncia a hechos por parte de cualquier tipo de organización social, que para el caso del presente trabajo se conforma como una denuncia de carácter ciudadano en la búsqueda de la defensa plena de los derechos humanos que le encubren para su desarrollo en una sociedad democrática.

## BIBLIOGRAFÍA


Adams, J., Khan, H. T. A., & Raeside, R. (2014). Introduction to research. *Research methods for business and social science students* (Second edition). Los Angeles: Sage.

Andrejevic, M. (2014). Big data, big questions: The big data divide. *International Journal of Communication, 8*, 17. Recuperado de http://ijoc.org/index.php/ijoc/article/view/2161

Ardèvol-Abreu, A. (2015). Framing o teoría del encuadre en comunicación: Orígenes, desarrollo y panorama actual en España. *Revista Latina De Comunicación Social,* (70), 423-450. doi:10.4185/RLCS-2015-1053

Arteaga Botello, N. (2015). Doing surveillance studies in Latin America: The insecurity context. *Surveillance & Society, 1*(13), 78-90. Recuperado de http://library.queensu.ca/ojs/index.php/surveillance-and-society/article/viewFile/lat/latinamerica

Barnard-Wills, D. (2011). UK media discourses of surveillance. *The Sociological Quarterly, 52*(4), 548-567. doi:10.1111/j.1533-8525.2011.01219.x

Bauman, Z., & Lyon, D. (2013). *Liquid surveillance*. Gran Bretaña: Polity.

Branum, J., & Charteris-Black, J. (2015). The Edward Snowden affair: A corpus study of the british press. *Discourse & Communication, 9*(2), 199-220. doi:10.1177/1750481314568544

Castells, M. (1999). Prólogo: La red y el yo. *La era de la información: Economía, sociedad y cultura* (pp. 27-53). México: Siglo XXI.

Cepik, M., & Ambros, C. (2014). Intelligence, crisis, and democracy: Institutional punctuations in Brazil, Colombia, South Africa, and India. *Intelligence and National Security, 29*(4), 523-551. doi:10.1080/02684527.2014.915176

Chong, D., & Druckman, J. N. (2007). Framing theory. *Annual Review of Political Science, 10*(1), 103-126. doi:10.1146/annurev.polisci.10.072805.103054

Cogo, D. (2011). Los estudios de recepción en América Latina: Perspectivas teórico-metodológicas. Recuperado de http://www.portalcomunicacion.com/lecciones_det.asp?id=48

Cortés Castillo, C. (2014). *Vigilancia de las comunicaciones en Colombia: El abismo entre la capacidad tecnológica y los controles legales*. Bogotá: Dejusticia.

Creswell, J. W. (1998). *Qualitative inquiry and research design: Choosing among five traditions*. London: Recuperado de http://catalog.hathitrust.org/Record/003184911

Department of Defense, United States. (2017). *DOD dictionary of military and associated terms*. Washington: Department of Defense, United States.

Dumas, J., & Roch, J. (2015). *Foundations of coding: Compression, encryption, error correction*. Somerset: Wiley. Recuperado de http://ebookcentral.proquest.com/lib/etech-trial/detail.action?docID=1895816

Durán Núnez, D. C. (2015). El software espía de la policía. *El Espectador.* Recuperado de http://www.elespectador.com/noticias/investigacion/el-software-espia-de-policia-articulo-571980

Dwyer, C., Hiltz, S. R., & Passerini, K.Trust and privacy concerns within social networking sites: A comparison of facebook and MySpace. *Americas Conference on Information Systems,* Colorado. 339.

Electronic Frontier Foundation. (2014). *International principles on the application of human rights to communications surveillance* (1st ed.). Estados Unidos: Electronic Frontier Foundation.

Elmer, G. (2012). Panopticon—discipline—control. *Routledge handbook of surveillance studies* (pp. 21-29). GB: Routledge Ltd - M.U.A. doi:10.4324/9780203814949

El Tiempo. (2017, 2 de Octubre). Polarización del país, reflejada en resultados del escrutinio. Recuperado de http://www.eltiempo.com/politica/proceso-de-paz/resultados-plebiscito-2016-42861

Fornaciari, F. (2014). *Privacy frames: How the media write, discuss, and afford privacy* Recuperado de http://indigo.uic.edu/handle/10027/19091

Fowler, R. (1991). *Language in the news : Discourse and ideology in the press*. London: Routledge. doi:10.4324/9781315002057

Fuchs, C. (2011a). How can surveillance be defined? *MATRIZes, 5*(1), 109. Recuperado de http://urn.kb.se/resolve?urn=urn:nbn:se:uu:diva-164479

Fuchs, C. (2011b). Towards an alternative concept of privacy. *Journal of Information, Communication and Ethics in Society, 9*(4), 220-237. doi:10.1108/14779961111191039

Fuchs, C. (2014). Social media and the public sphere. *tripleC, 12*(1), 57-101. Recuperado de http://www.triple-c.at/index.php/tripleC/article/view/552

Fundación Karisma. (2016). ¿Qué hay de nuevo en el estado de vigilancia masiva de Colombia? Recuperado de https://karisma.org.co/que-hay-de-nuevo-en-el-estado-de-la-vigilancia-masiva-en-colombia/

Gamson, W. A., & Modigliani, A. (1987). The changing culture of affirmative action. In R. G. Braungart, & M. M. Braungart (Eds.), *Research in political sociology* (pp. 137-177). Greenwich, Connecticut: JAI Press.

Gee, J. P., & Handford, M. (2012). *The Routledge handbook of discourse analysis*. GB: Routledge Ltd - M.U.A. doi:10.4324/9780203809068

Ghanem, S. I. (1997). El segundo nivel de composición de la agenda: la opinión pública y la cobertura del crimen. *Comunicación y sociedad: Revista de la Facultad de Comunicación, 10*(1), 151-167. Recuperado de http://dialnet.unirioja.es/servlet/oaiart?codigo=4490667

Gilgun, J. F. (2015). Beyond description to interpretation and theory in qualitative social work research. *Qualitative Social Work, 14*(6), 741-752. doi:10.1177/1473325015606513

Gómez Mendoza, M. Á. (2000). Análisis de contenido cualitativo y cuantitativo: Definición, clasificación y metodología. *Revista De Ciencias Humanas,* (20), 129-138.

Griffin, A. (2016, Jan 19,). Facebook launches "initiative for civil courage online" to delete racist and threatening posts. *Independent* Recuperado de http://www.independent.co.uk/life-style/gadgets-and-tech/news/facebook-launches-initiative-for-civil-courage-online-to-delete-racist-and-threatening-posts-a6821581.html

Grupo de Memoria Histórica. (2013). *¡Basta ya! Colombia: Memorias de guerra y dignidad*. Bogotá: Centro Cultural de Memoria Histórica.

Habermas, J. (1997). La transformación social de la estructura de la publicidad. In J. Habermas (Ed.), *Historia y crítica de la opinión pública: La transformación estructural de la vida pública* (pp. 172-208). España: Gustavo Gili, S.A.

Hosein, G. (2014). Going dark? the rule of law, the iPhone, and closet doors. Recuperado de https://www.privacyinternational.org/?q=node/449

Human Rights Watch. (2017). *Colombia: Eventos del 2016*. New York: Human Rights Watch. Recuperado de https://www.hrw.org/es/world-report/country-chapters/298516

Jensen, K. B. (2012). *A handbook of media and communication research* (2nd ed.). Gran Bretaña: Routledge Ltd - M.U.A. doi:10.4324/9780203357255

John, N. A., & Peters, B. (2017). Why privacy keeps dying: The trouble with talk about the end of privacy. *Information, Communication & Society, 20*(2), 284-298. doi:10.1080/1369118X.2016.1167229

Kerr, I., & Barrigar, J. (2012). Privacy, identity and anonymity. In K. Ball, K. Taggerty & D. Lyon (Eds.), *Routledge handbook of surveillance studies* (pp. 386-394). New York: Routledge.

Khalil, C. (2015). Thinking intelligently about intelligence: A model global framework protecting privacy. *The George Washington International Law Review, 47*(4), 919-947. Recuperado de https://search.proquest.com/docview/1802711984?accountid=174072

Kumpu, V. (2012). Privacy and the emergence of the "ubiquitous computing society": The struggle over the meaning of "privacy" in the case of the apple location tracking scandal. *Technology in Society, 34*(4), 303-310. doi:10.1016/j.techsoc.2012.10.002

Lash, S. (2007). Power after hegemony. *Theory, Culture & Society, 24*(3), 55-78.

Lischka, J. A. (2017). Explicit terror prevention versus vague civil liberty: How the UK broadcasting news (de)legitimatise online mass surveillance since Edward

Snowden's revelations. *Information, Communication & Society, 20*(5), 665. doi:10.1080/1369118X.2016.1211721

Lyon, D., Haggerty, K., & Ball, K. (2012). Introducing surveillance studies. In D. Lyon, K. Haggerty & K. Ball (Eds.), *Routledge handbook of surveillance studies* (pp. 1-12). Londres: Routledge.

Manetto, F. (2017). Los cultivos de coca en Colombia aumentaron más del 50% en 2016. Recuperado de https://elpais.com/internacional/2017/07/15/colombia/1500075179_746891.html

Mariño, M. V. Desde el análisis de contenido hacia el análisis del discurso: La necesidad de una apuesta decidida por la triangulación metodológica; *IX Congreso Iberoamericano De Comunicación,*

Martín-Barbero, J. (2005). Globalização comunicacional e transformação cultural. In D. Moraes (Ed.), *Por uma outra comunicação* (pp. 57-88). Rio de Janeiro: Record.

Marx, G. T. (2007). Surveillance. In W. Staples (Ed.), *Encyclopedia of privacy* (pp. 535-544). Estados Unidos: Greenwood Press.

Marx, G. T. (2016). *Windows into the soul: Surveillance and society in an age of high technology*. Chicago: University Of Chicago Press. Recuperado de http://replace-me/ebraryid=11213100

Mason, P. (2016). *Postcapitalismo: Hacia un nuevo futuro*. España: Ediciones Paidós.

Mayer-Schonberger, V., & Cukier, K. (2013). Datification. *Big data: A revolution that will transform how we live, work and think* (). Great Britain: Jhon Murray.

Mayring, P. (2014). *Qualitative content analysis: Theoretical foundation, basic procedures and software solution*. Klagenfurt: AUT.

McCombs, M., & Ghanem, S. (2001). The convergence of agenda setting and framing. *Framing public life: Perspectives on media and our understanding of the social world* (pp. 67-82). Mahwah, NJ: Lawrence Erlbaum Associates.

McCombs, M. E., & Shaw, D. L. (1972). The agenda-setting function of mass media. *The Public Opinion Quarterly, 36*(2), 176-187.

Nissenbaum, H. (2010). *Privacy in context: technology, policy, and the integrity of social life*. Stanford: Stanford Law Books.

Noain Sánchez, A. (2015). La privacidad como integridad contextual y su aplicación a las redes sociales. *Zer - Revista De Estudios De Comunicación, 20*(39), 163-175. doi:10.1387/zer.15531

Oller Alonso, M. (2014). The triangle formed by framing, agenda-setting and metacoverage. *Disertaciones: Anuario Electrónico De Estudios En Comunicación Social, 7*(1), 41-66. Recuperado de http://dialnet.unirioja.es/servlet/oaiart?codigo=4800926

Organización de las Naciones Unidas. (2014). Mass surveillance: Exceptional measure or dangerous habit? Recuperado de http://www.ohchr.org/EN/NewsEvents/Pages/MassSurveillance.aspx

Organización de las Naciones Unidas. (2015). La declaración universal de derechos humanos. Recuperado de http://www.un.org/es/universal-declaration-human-rights/

Parliament of United Kingdom. (2009). Chapter 2: Overview of surveillance and data collection. *Surveillance: Citizens and the state* (pp. 11-19). London: House of Lords. Recuperado de http://www.publications.parliament.uk/pa/ld200809/ldselect/ldconst/18/18.pdf

Patton, M. Q. (2002). Two decades of developments in qualitative inquiry. *Qualitative Social Work, 1*(3), 261-283. doi:10.1177/1473325002001003636

Pérez de Acha, G. (2016, -09-05). El auge del software de vigilancia en América Latina. *Elespectador.Com* Recuperado de http://www.elespectador.com/tecnologia/el-auge-del-software-de-vigilancia-america-latina-articulo-653099

Pérez, C. (2012). Revoluciones tecnológicas y paradigmas tecnoeconómicos. *Tecnología Y Construcción, 21*(1) Recuperado de https://scholar.google.cl/scholar?hl=en&q=Revoluciones+tecnol%C3%B3gicas+y+paradigmas+tecnoecon%C3%B3micos&btnG=&as_sdt=1%2C5&as_sdtp=

Privacy International. (2015a). *Demanda y oferta: La industria de la vigilancia al descubierto.* Lóndres: Privacy International.

Privacy International. (2015b). *Un estado en la sombra: Vigilancia y orden público en Colombia.* Lóndres: Privacy International.

República de Colombia (2011). *Ley 1448: Ley de víctimas y restitución de tierras*.

República de Colombia. (2017). *Radiografía de venezolanos en Colombia*. Colombia: Ministerio de Relaciones Exteriores.

Revista Semana (2009). El DAS sigue grabando. Recuperado de http://www.semana.com/nacion/articulo/el-das-sigue-grabando/100370-3

Revista Semana (2017). El fantasma del castrochavismo. Recuperado de http://www.semana.com/nacion/articulo/colombianos-creen-que-el-pais-se-puede-convertir-en-venezuela/528035

Rider, K. (2016). *The privacy paradox: Privacy, surveillance, and encryption* (Master's). Available from ProQuest Dissertations & Theses A&I, ProQuest

Dissertations & Theses Global. (1844057945). Recuperado de https://search.proquest.com/docview/1844057945?accountid=174072

Rodríguez Gómez, G., Gil Flores, J., & García Jiménez, E. (1996). Métodos de investigación cualitativa. In G. Rodríguez Gómez, J. Gil Flores & E. García Jiménez (Eds.), *Metodología de la investigación cualitativa* (pp. 39-59). Málaga, España: Ediciones Aljibe.

Rodríguez, K. (2012). Colombia adopts mandatory backdoor and data retention mandates. Recuperado de https://www.eff.org/deeplinks/2012/12/cultures-secrecy-colombia-adopts-mandatory-backdoor-and-data-retention-mandates

Roznowski, J. L. (2003). A content analysis of mass media stories surrounding the consumer privacy issue 1990-2001. *Journal of Interactive Marketing, 17*(2), 52-69. doi:10.1002/dir.10054

Scheufele, D. A., & Tewksbury, D. (2007). Framing, agenda setting, and priming: The evolution of three media effects models. *Journal of Communication, 57*(1), 9-20. doi:10.1111/j.1460-2466.2006.00326.x

Snowden, E., Poitras, L., & Greenwald, G. (2013, ). NSA whistleblower Edward Snowden: 'I don't want to live in a society that does these sort of things' [video]. *The Guardian* Recuperado de http://www.theguardian.com/world/video/2013/jun/09/nsa-whistleblower-edward-snowden-interview-video

Solove, D. (2010). The meaning and value of privacy. In J. Seijdel, & L. Melis (Eds.), *Beyond privacy: New perspectives on the public and private domain* (pp. 35-43). Rotterdam: NAi Publishers.

Sosa Troya, M. (2015). ¿Cómo legislan los gobiernos sobre vigilancia masiva? Recuperado de

http://internacional.elpais.com/internacional/2015/06/05/actualidad/1433515872_277281.html

Stahl, T. (2016). Indiscriminate mass surveillance and the public sphere. *Ethics and Information Technology, 18*(1), 33-39. doi:10.1007/s10676-016-9392-2

Sveiby, K., Gripenberg, P., & Segercrantz, B. (2012). Challenging the innovation paradigm: The prevailing pro-innovation bias. In K. Sveiby, P. Gripenberg & B. Segercrantz (Eds.), *Challenging the innovation paradigm* (pp. 1-12). London: Routledge. doi:10.4324/9780203120972

Tavani, H. T. (2008). Informational privacy: Concepts, theories, and controversies. In K. E. Himma, & H. T. Tavani (Eds.), *The handbook of information and computer ethics* (pp. 131-164). Hoboken, New Jersey: Wiley.

Taylor, S. J., Bogdan, R., & DeVault, M. L. (2016). *Introduction to qualitative research methods* (Fourth edition ed.). Hoboken, New Jersey: Wiley.

Vasilachis de Gialdino, I. (2006). La investigación cualitativa. In I. Vasilachis de Gialdino, A. R. Ameigeiras, L. B. Chernobilsky, V. Giménez Béliveau, F. Mallimaci, N. Mendizábal, A. J. Soneira (Eds.), *Estrategias de investigación cualitativa* (pp. 23-30). Barcelona: Gedisa.

Wall, D. (2007). *Cybercrime*. Cambridge: Polity.

# ANEXOS

## Anexo I. Listado de informes sobre vigilancia estatal en Colombia y Latinoamérica

| AUTORÍA | TÍTULO | FECHA | URL |
|---|---|---|---|
| **Electronic Frontier Foundation; Fundación Karisma; Comisión Colombiana de Juristas** | Vigilancia estatal de las comunicaciones y protección de los derechos fundamentales en Colombia | Mar-16 | https://necessaryandproportionate.org/es/country-reports/colombia |
| **Álvarez Ugarte, Ramiro** | El caso Snowden y la democracia en disputa | Sep-13 | http://nuso.org/media/articles/downloads/3975_1.pdf |
| **Fundación Karisma; Electronic Frontier Foundation** | ¿Dónde están mis datos?: Buscando la transparencia de los intermediarios de Internet en Colombia | Nov-16 | http://dondeestanmisdatos.info/2016/download/donde-estan-mis-datos-2016.pdf |
| **Electronic Frontier Foundation; Fundación Karisma; Comisión Colombiana de Juristas** | Vigilancia de las comunicaciones por la autoridad y protección de los derechos fundamentales en Colombia | May-15 | https://www.eff.org/files/2015/05/21/vigilancia_de_comunicaciones_colombia_eff.pdf |
| **Privacy International** | Demanda y oferta: la industria de la vigilancia al descubierto | Jul-15 | https://www.privacyinternational.org/sites/default/files/DemandSupply_Espanol.pdf |
| **Privacy International; Fundación Karisma; Dejusticia** | The Right to Privacy in Colombia | Mar-16 | https://www.privacyinternational.org/sites/default/files/HRC_colombia.pdf |
| **Privacy International** | Un estado en la sombra: vigilancia y orden público en Colombia | Aug-15 | https://www.privacyinternational.org/sites/default/files/ShadowState_Espanol.pdf |
| **Derechos Digitales** | Hacking Team: Malware para la vigilancia en América Latina | Mar-16 | https://www.derechosdigitales.org/wp-content/uploads/malware-para-la-vigilancia.pdf |
| **Fundación Karisma** | Escucha perspectivas latinoamericanas frente al análisis de datos y vigilancia estatal | Nov-16 | https://karisma.org.co/escuchalatam/ |
| **Fundación Karisma; Privacy International** | Big Data: un aporte para la discusión de la política pública en Colombia | Nov-16 | https://karisma.org.co/big-data-un-aporte-para-la-discusion-de-la-politica-publica-en-colombia/ |
| **Fundación Karisma** | ¿Es legítima la retención de datos en Colombia? Análisis comparativo de una herramienta de vigilancia masiva que restringe los derechos humanos | Jan-16 | https://karisma.org.co/es-legitima-la-retencion-de-datos-en-colombia/ |
| **Fundación Karisma; Privacy International** | Cuando el estado "Hackea": análisis de la legitimidad del uso de herramientas de hacking en Colombia | Dec-15 | https://karisma.org.co/cuando-el-estado-hackea-3/ |
| **Dejusticia** | Vigilancia de las comunicaciones en Colombia: el abismo entre la capacidad tecnológica y los controles legales | Jul-14 | https://www.dejusticia.org/wp-content/uploads/2017/04/fi_name_recurso_643.pdf |
| **Privacy International; Fundación Karisma; Dejusticia** | State of privacy Colombia | Mar-17 | https://privacyinternational.org/node/977 |

## Anexo II. Dimensiones de la vigilancia tradicional y la nueva vigilancia (Marx, 2016)

| DIMENSION | TRADITIONAL SURVEILLANCE | NEW SURVEILLANCE |
|---|---|---|
| **Senses** | Unaided senses | Extends senses, new kinds of sensing |
| **Visibility (literally or known about)** | Visible | Less visible or invisible |
| **Consent** | Lower proportion involuntary | Higher proportion involuntary |
| **Cost** | Expensive per-unit data | Inexpensive per-unit data |
| **Location of data collectors or analyzers** | On scene | Remote |
| **Fixity of data collection** | Stationary | Stationary, roams |
| **Ethos** | Harder (more coercive) | Softer (less coercive) |
| **Integration** | Data collection as separate activity | Data collection folded into routine activity |
| **Data collector** | Animate (human, animal) | Machine |
| **Operation** | Manual | Automated |
| **Time lag between data collection and action based on it** | Yes | No, can be immediate |
| **Attached to person or objetct** | No | Can be |
| **Where data resides** | With the collector, stays local | With third parties, often migrates |
| **Timing** | Single point or intermittent | Continuous, omnipresent |
| **Time period** | Present | Past, present, future |
| **Data availability** | Frequent time lags | Real-time availability |
| **Technology availability** | Disproportionately available to elites | More democratized, some forms widely available |
| **Focus of data collection** | Individual | Individual, categories of interest, objects |
| **Comprehensiveness** | Single measure | Multiple measures |
| **Context** | Contextual | Acontextual |
| **Depth** | Less intensive | More intensive |
| **Breadth** | Less extensive | More extensive |
| **Ratio of surveillant to self-knowledge** | Higher (what the surveillant knows, the subject more likely knows as well) | Lower (surveillant more likely knows things subject doesn't) |
| **Identifiability of subject of surveillance** | Emphasis on knows individuals | Emphasis also on anonymous individuals, masses |
| **Emphasis** | Individuals | Individuals, networks, systems |
| **Data appearance** | Direct representation | Realistic, abstracted, indirect, simulated |
| **Form** | Single media (narrative or numerical) | Multiple media |

| | | |
|---|---|---|
| **Who collects data** | Specialists | Specialists, role dispersal, self-monitoring |
| **Where collected** | Encloses, bounded space | Bounded or open |
| **Ease of data analysis** | More difficult to organize, store, retrieve, analyze | Easier to organize, store, retrieve, analyze |
| **Extent of data merging** | Discrete, noncombinable | Easy to combine because digitized |
| **Ease of data communication** | More difficult to send | Easier to send, receive |
| **Documentation, record keeping, searching** | Requires additional steps, less routine | Inherent in the process or routinely done |
| **Basis of judgements** | The unique individual | The individual in relation to statistical averages and aggregate categories |

## Anexo III. Corpus de noticias

| TÍTULO | FECHA | PERIÓDICO |
|---|---|---|
| ¿Argentina, en la mira de los ingleses? | Jun 4, 2015 | El Espectador |
| ¿Colombia está chuzada? | Jul 10, 2015 | El Espectador |
| ¿Quién controla las puertas traseras? | Feb 25, 2016 | El Espectador |
| 'El galeón San José está bien custodiado' | Jan 4, 2016 | El Tiempo |
| "Equiparar un monitoreo con chuzadas es una canallada": Hollman Morris | Nov 28, 2016 | El Espectador |
| "La Policía necesita más legitimidad": general Jorge Nieto | Feb 20, 2016 | El Espectador |
| "No hay duda de los seguimientos": Vicky Dávila | Dec 4, 2015 | El Espectador |
| "Se debe indagar el alcance de los sistemas de vigilancia de la Policía" | Aug 30, 2015 | El Espectador |
| "Todo se puede monitorear" | Jul 25, 2015 | El Espectador |
| Al DAS también le ofrecieron el cuestionado software espía | Jul 18, 2015 | El Espectador |
| Alianzas con privados, fórmula para enfrentar crisis carcelaria | May 25, 2015 | El Tiempo |
| Anonymous convoca multitudinarias marchas para conmemorar el 5 de noviembre | Nov 5, 2015 | El Espectador |
| Avanza política de seguridad digital | Feb 4, 2016 | El Espectador |
| Bogotá duplicará sus cámaras de seguridad | Jul 14, 2016 | El Espectador |
| Cartagenera extorsionaba a su novio a través de WhatsApp | Mar 3, 2015 | El Espectador |
| Comienzan las pruebas a sistema de interceptación | Sep 30, 2015 | El Tiempo |
| Cómo Flash pasó de ser un estándar de la red a una herramienta casi muerta | Dec 21, 2015 | El Espectador |
| Cómo los celulares se volvieron el blanco perfecto para las agencias de seguridad | Sep 5, 2016 | El Espectador |
| CTI de la jurisdicción castrense podrá intervenir comunicaciones | Jul 27, 2015 | El Tiempo |
| Cuestionan a firma de contrato de brazaletes | Dec 29, 2016 | El Tiempo |
| Defensa de Napout pide más tiempo para reunir dinero de fianza | Dec 23, 2015 | El Espectador |
| Desde EE.UU. hasta Australia, policías van a la caza del "Chapo" Guzmán: DEA | Jul 30, 2015 | El Espectador |
| Detalles de cómo la Procuraduría decidió abrir una investigación contra Palomino | Feb 16, 2016 | El Espectador |
| Director latino de Facebook dice que ''no tienen cómo vender bases de datos'' | Apr 24, 2015 | El Espectador |
| EE.UU. dice no tener "interés ni intención de desestabilizar" Venezuela | Nov 19, 2015 | El Espectador |
| El auge del software de vigilancia en América Latina | Sep 5, 2016 | El Espectador |
| El dilema de los datos personales | May 20, 2015 | El Espectador |
| El Estado Islámico y el debate sobre la encriptación | Nov 18, 2015 | El Espectador |
| El fin de la vigilancia masiva de la NSA | Jun 2, 2015 | El Espectador |
| El hackeador hackeado | Jul 10, 2015 | El Espectador |

| | | |
|---|---|---|
| El hombre que sabía demasiado | Feb 4, 2015 | El Espectador |
| El nuevo servicio de Messenger de Facebook que le permitirá tener conversaciones secretas | Jul 8, 2016 | El Espectador |
| El paso de 'Juancho Prada' por las Autodefensas | Feb 11, 2015 | El Espectador |
| El plan de gobierno de Clara López | Oct 22, 2015 | El Espectador |
| El pulso entre la seguridad y la privacidad | Jun 3, 2015 | El Espectador |
| El software espía de la Policía | Jul 11, 2015 | El Espectador |
| Emergencia carcelaria para superar crisis en salud en las cárceles | May 6, 2016 | El Tiempo |
| En defensa del cifrado | Nov 19, 2015 | El Espectador |
| En libertad uno de los hermanos 'Comba' | Feb 1, 2016 | El Espectador |
| Entre el terror y la encriptación | Nov 18, 2015 | El Espectador |
| Error de capa 8 | Sep 10, 2015 | El Espectador |
| Espiar sin control de un juez, la apuesta francesa | May 6, 2015 | El Tiempo |
| Estas son las tres plataformas utilizadas para interceptar en Colombia según la Flip | Dec 9, 2015 | El Espectador |
| Estos son los retos a los que se enfrenta internet actualmente | May 17, 2016 | El Espectador |
| Europa golpea a gigantes digitales | Oct 13, 2015 | El Tiempo |
| Europa pasa al ataque | Oct 6, 2015 | El Espectador |
| Fiscalía estadounidense se opone a pedido de Napout de libertad bajo fianza | Feb 24, 2016 | El Espectador |
| Inpec: en un año, 189 presos en domiciliaria y con brazaletes se fugaron | Feb 5, 2015 | El Tiempo |
| Inteligencia en Colombia: el reino de las sombras | Aug 29, 2015 | El Espectador |
| Inteligencia: el reino de las sombras | Aug 29, 2015 | El Espectador |
| Intentan prohibir inversión extranjera en seguridad privada | Apr 7, 2015 | El Tiempo |
| Investigadores arrojan luz sobre el origen del software malicioso | Jun 16, 2016 | El Espectador |
| Investigan posible daño patrimonial en contrato de brazaletes electrónicos | Jul 7, 2016 | El Espectador |
| La delgada línea entre una herramienta y un arma | Apr 14, 2015 | El Espectador |
| La encriptación como derecho | Jul 26, 2015 | El Espectador |
| La expansión de las operaciones de la NSA | Jun 4, 2015 | El Espectador |
| La Justicia Especial para la Paz, según Minjusticia | Dec 18, 2016 | El Tiempo |
| La moral según Facebook | Mar 8, 2015 | El Espectador |
| La ONU, Colombia y la vida privada | Nov 11, 2016 | El Espectador |
| La regresión de Rafael Correa | Sep 8, 2015 | El Espectador |
| La rutina global de controlar la información | Aug 13, 2015 | El Espectador |
| Las chuzadas no volvieron: nunca se fueron | Dec 12, 2015 | El Espectador |
| Las mejores empresas para la privacidad de sus usuarios | Jun 18, 2015 | El Espectador |

| | | |
|---|---|---|
| Lecciones del hackeo a la NSA | Aug 18, 2016 | El Espectador |
| Los reparos de Human Rights Watch a la ley de amnistía | Dec 26, 2016 | El Espectador |
| Los socios detrás del ganador de la puja por peajes | Jul 1, 2016 | El Tiempo |
| Malware de Gobierno | Jul 23, 2015 | El Espectador |
| Más de 8.500 detenidos saldrán de prisión | Jul 7, 2016 | El Espectador |
| Más tecnologías para la seguridad de los aeropuertos | May 20, 2015 | El Espectador |
| No solo tenemos pumas, tenemos "super pumas" | Sep 3, 2015 | El Espectador |
| Otorgan detención domiciliaria al excongresista Germán Olano | May 6, 2015 | El Espectador |
| Puerto Rico inicia cultivo y venta de cannabis medicinal | Jan 28, 2016 | El Espectador |
| Rechazo a acuerdo de paz casi que aniquila la posibilidad de un Nobel de la paz | Oct 3, 2016 | El Espectador |
| Rechazo al acuerdo de paz casi que aniquila la posibilidad de un Nobel de la paz | Oct 3, 2016 | El Espectador |
| Reclusión con fiestas, salidas y hasta Play Station | Sep 16, 2015 | El Tiempo |
| Star Trek, el boom de Cómic-Con | Jul 21, 2016 | El Espectador |
| Todos somos culpables | Mar 10, 2015 | El Espectador |
| Un Estado de la UE puede suspender envío de datos de Facebook a EE.UU. | Sep 23, 2015 | El Espectador |
| Un millón de dólares por hacer jailbreak de iOS | Nov 4, 2015 | El Espectador |
| Un mundo de chuzadas | Jul 22, 2015 | El Espectador |
| Violencia contra defensores de DD.HH.: 63 asesinados en 2015 | Mar 2, 2016 | El Espectador |
| WikiLeaks amenaza con sacudir elecciones en EE. UU. | Oct 5, 2016 | El Tiempo |
| Wikileaks vincula a Policía australiana con empresas de espionaje electrónico | Jul 9, 2015 | El Espectador |

## Anexo IV. Listado de categorías

| POSICIÓN | FRECUENCIA | PALABRA | POSICIÓN | FRECUENCIA | PALABRA |
|---|---|---|---|---|---|
| **1** | 213 | policía | **39** | 55 | político |
| **2** | 190 | vigilancia | **40** | 50 | control |
| **3** | 169 | información | **41** | 47 | privacidad |
| **4** | 156 | seguridad | **42** | 43 | protección |
| **5** | 149 | derecho | **43** | 39 | delito |
| **6** | 129 | país | **44** | 38 | cámara |
| **7** | 125 | empresa | **45** | 38 | facebook |
| **8** | 117 | comunicación | **46** | 37 | ilegal |
| **9** | 116 | inteligencia | **47** | 36 | correo |
| **10** | 116 | sistema | **48** | 36 | denunciar |
| **11** | 111 | gobierno | **49** | 36 | nsa |
| **12** | 105 | dato | **50** | 36 | personal |
| **13** | 98 | público | **51** | 35 | poder |
| **14** | 93 | hacking | **52** | 35 | controlar |
| **15** | 91 | team | **53** | 35 | espionaje |
| **16** | 87 | masivo | **54** | 33 | corte |
| **17** | 86 | tratado-ley | **55** | 33 | snowden |
| **18** | 82 | herramienta | **56** | 31 | ataque |
| **19** | 82 | servicio | **57** | 31 | interceptar |
| **20** | 81 | software | **58** | 30 | monitoreo |
| **21** | 81 | tecnología | **59** | 29 | defensa |
| **22** | 79 | nacional | **60** | 29 | orden |
| **23** | 71 | fiscalía | **61** | 29 | teléfono |
| **24** | 70 | documento | **62** | 28 | celular |
| **25** | 69 | ciudadano | **63** | 28 | computador |
| **26** | 68 | libertar | **64** | 28 | transparencia |
| **27** | 65 | colombiano | **65** | 27 | amenazar |
| **28** | 65 | humano | **66** | 25 | tribunal |
| **29** | 65 | usuario | **67** | 24 | capturar |
| **30** | 64 | digital | **68** | 24 | informático |
| **31** | 63 | privar | **69** | 24 | ministerio |
| **32** | 63 | red | **70** | 24 | principio |
| **33** | 62 | electrónico | **71** | 23 | chuzadas |
| **34** | 62 | interceptación | **72** | 23 | secreto |
| **35** | 59 | internet | **73** | 22 | penal |
| **36** | 58 | programar | **74** | 21 | encriptación |
| **37** | 57 | autoridad | **75** | 21 | palomino |
| **38** | 57 | legal | **76** | 21 | privacy |
| **77** | 21 | rcs | **115** | 13 | telefónico |
| **78** | 20 | comunicar | **116** | 13 | violación |
| **79** | 20 | escándalo | **117** | 12 | acusar |
| **80** | 20 | italiano | **118** | 12 | congreso |
| **81** | 20 | proteger | **119** | 12 | contraloría |
| **82** | 20 | víctima | **120** | 12 | google |
| **83** | 20 | vigilar | **121** | 12 | malware |
| **84** | 19 | blanco | **122** | 12 | metadatos |
| **85** | 19 | esperanzar | **123** | 12 | senador |

| POSICIÓN | FRECUENCIA | PALABRA |
|---|---|---|
| **86** | 18 | inpec |
| **87** | 18 | robotec |
| **88** | 17 | penar |
| **89** | 17 | político-jurídico |
| **90** | 16 | constitucional |
| **91** | 16 | filtración |
| **92** | 16 | legislación |
| **93** | 16 | prisión |
| **94** | 15 | ley |
| **95** | 15 | procuraduría |
| **96** | 15 | tecnológico |
| **97** | 15 | wikileaks |
| **98** | 14 | civil |
| **99** | 14 | detectar |
| **100** | 14 | galileo |
| **101** | 14 | identificar |
| **102** | 14 | legítimo |
| **103** | 14 | posconflicto |
| **104** | 14 | preocupación |
| **105** | 14 | recolectar |
| **106** | 14 | regular |
| **107** | 14 | seguro |
| **108** | 14 | terrorismo |
| **109** | 13 | contratación |
| **110** | 13 | espía |
| **111** | 13 | espiar |
| **112** | 13 | malicioso |
| **113** | 13 | operador |
| **114** | 13 | opositor |

| POSICIÓN | FRECUENCIA | PALABRA |
|---|---|---|
| **124** | 12 | sociedad |
| **125** | 11 | comunidad |
| **126** | 11 | hackeo |
| **127** | 11 | intimidar |
| **128** | 11 | jailbreak |
| **129** | 11 | senado |
| **130** | 10 | human |
| **131** | 10 | jurisdicción |
| **132** | 10 | peligro |
| **133** | 10 | rastrear |
| **134** | 10 | recolección |
| **135** | 10 | rights |
| **136** | 10 | telecomunicación |
| **137** | 10 | whatsapp |

# PAUTA DE EVALUACIÓN
# MAGISTER EN COMUNICACIÓN SOCIAL

**Título: Agenda de la prensa escrita digital respecto a los temas de la privacidad de la ciudadanía y la vigilancia estatal en Colombia durante el período 2015-2016: sistemas de vigilancia estatal y el caso Hacking Team.**
**Autor/a:**

**Profesor/a Guía: María Cecilia Bravo Núñez**
**Profesor/a Informante:**

| ASPECTOS A EVALUAR |
|---|
| **1. FORMULACIÓN Y FUNDAMENTACIÓN DEL PROBLEMA** |
| • El problema está planteado de manera precisa y coherente.<br>• La pregunta de investigación se desprende coherentemente de los antecedentes del problema planteados.<br>• Se justifica en forma adecuada la relevancia del problema a investigar y el aporte de la investigación al campo de la comunicación |
| **2. OBJETIVOS** |
| • El objetivo general del proyecto está formulado en forma clara, precisa y coherente, desprendiéndose de la pregunta de investigación.<br>• Los objetivos específicos del proyecto son formulados explícitamente, se detallan los contenidos del objetivo general y se mantiene la coherencia con la pregunta de investigación. |
| **3. MARCO DE REFERENCIA TEÓRICO** |
| • El marco de referencia presenta un conjunto de teorías generales que abordan el problema de investigación.<br>• El marco de referencia presenta un conjunto de antecedentes teórico-empíricos actualizados, directamente vinculados al problema de la investigación.<br>• El marco de referencia se organiza de manera lógica y refleja una elaboración por parte del (a) alumno(a) y no una simple enumeración de teorías. |
| **4. MARCO DE REFERENCIA METODOLÓGICO** |
| • El enfoque metodológico está adecuadamente definido y justificado, es coherente con el problema de investigación y mantiene relación con el logro de los objetivos.<br>• Adecuada definición de los conceptos teóricos y/o variables de la investigación.<br>• El universo y/o el tipo muestral está bien definido, caracterizado, y es coherente con el problema y objetivos de estudio.<br>• Las técnicas de producción de datos se encuentra adecuadamente identificadas y definidas, manteniendo coherencia con el enfoque metodológico.<br>• Las técnicas de análisis de datos, se encuentran definidas y caracterizadas, son adecuadas a los objetivos de la investigación y son pertinentes con el enfoque metodológico.<br>• Se justifica la validez, confiabilidad y/o calidad del diseño metodológico. |

**5. ANÁLISIS Y/0 DISCUSIÓN DE RESULTADOS**

- El análisis de datos presentado está adecuadamente desarrollado y es pertinente a la producción de datos, manteniendo coherencia con los objetivos de la investigación.
- La discusión de los datos se relaciona con el marco de referencia teórico.
- Se utilizan las citas textuales y/o numéricas de los datos en forma integrada al texto de análisis.

**6. CONCLUSIONES, SUGERENCIAS Y PROYECCIONES**

- Las conclusiones reflejan la unidad de todo el proceso de investigación.
- Las conclusiones se presentan en forma clara y coherente con el análisis y los objetivos planteados.
- Las sugerencias se desprenden de las conclusiones y el proceso analítico presentado.
- Presenta sugerencias teóricas, metodológicas y/o prácticas proponiendo nuevas líneas y/o temas de investigación.
- Se indican proyecciones adecuadas y relacionadas con la investigación desarrollada en el contexto del área específica o campo de la comunicación.

**7. BIBLIOGRAFÍA**

- La bibliografía es relevante en cuanto a la calidad de los textos y fuentes seleccionados, y pertinente en relación al problema de investigación y/o al área de especialización.
- Todos los textos o fuentes citados en el desarrollo de la Memoria se encuentran debidamente registrados en la Bibliografía.
- Todas las citas se presentan de acuerdo a alguna de las normas comúnmente aceptadas para trabajos científicos.

**8. ASPECTOS FORMALES**

- El título sintetiza en forma clara y comprensiva el principal propósito de la investigación.
- Se respetan normas gramaticales y ortográficas.
- La redacción es adecuada.
- Presenta índice, siglas, identifica al autor/a y Profesor/a Guía.

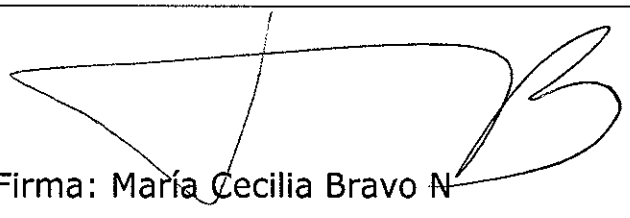
# ESCALA PARA CALIFICAR MEMORIA DE GRADO

| | ITEM EVALUADO | PUNTAJES | | | | | | | | multiplicar por | PUNTAJE |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | Formulación y Fundamentación de problema | 1 | 2 | 3 | 4 | 5 | 6 | **7** | | 0.10 | **0.7** |
| | | | | | | | | | | | |
| 2 | Objetivos | 1 | 2 | 3 | 4 | 5 | 6 | **7** | | 0,05 | **0.35** |
| | | | | | | | | | | | |
| 3 | Marco de Referencia Teórico | 1 | 2 | 3 | 4 | 5 | **6.5** | 7 | | 0.20 | **1.3** |
| | | | | | | | | | | | |
| 4 | Marco de Referencia Metodológico | 1 | 2 | 3 | 4 | 5 | 6 | **7** | | 0.15 | **1.05** |
| | | | | | | | | | | | |
| 5 | Resultados (Análisis y Discusión) | 1 | 2 | 3 | 4 | 5 | 6 | **7** | | 0.20 | **1.4** |
| | | | | | | | | | | | |
| 6 | Conclusiones | 1 | 2 | 3 | 4 | 5 | 6 | **7** | | 0.15 | **1.05** |
| | | | | | | | | | | | |
| 7 | Bibliografía | 1 | 2 | 3 | 4 | 5 | **6.5** | 7 | | 0.10 | **0.65** |
| | | | | | | | | | | | |
| 8 | Aspectos formales | 1 | 2 | 3 | 4 | 5 | 6 | **7** | | 0.05 | **0.35** |

**6.9**

PTJE FINAL

| INFORME DE EVALUACIÓN |
|---|
| |
| **1. FORMULACIÓN Y FUNDAMENTACIÓN DEL PROBLEMA** |
| La formulación y fundamentación del problema es clara y pertinente- |
| **2. OBJETIVOS** |
| Los objetivos están directa relación con la pregunta general que aborda el tema de investigación propuesto. El objetivo general da cuenta del fin que tiene la investigación. |
| **3. MARCO DE REFERENCIA TEÓRICO** |
| Se sugiere abordar el tema de medios y de agenda setting con mayor profundidad. |
| **4. MARCO DE REFERENCIA METODOLÓGICO** |
| Es coherente con el problema, preguntas y objetivos. |
| **5. ANÁLISIS Y DISCUSIÓN DE RESULTADOS** |
| Los resultados da cuenta de un trabajo acucioso de parte del estudiante. |
| **6. CONCLUSIONES** |
| Aborda los aspectos centrales de los resultados y propone nuevas aristas que pueden ser investigadas en investigaciones parecidas. |
| **7. BIBLIOGRAFÍA** |
| Bien. |
| |
| **8. ASPECTOS FORMALES** |
| Bien |
| **9. OBSERVACIONES** |
| |



Nombre y Firma: María Cecilia Bravo N

Fecha: Marzo, 2018

# PAUTA DE EVALUACIÓN
# MAGISTER EN COMUNICACIÓN SOCIAL

**Título:** Agenda de la prensa escrita digital respecto de los temas de la privacidad de la ciudadanía y vigilancia estatal en Colombia en el período 2015-2016: sistemas de vigilancia estatal y el caso "Hacking Team"
**Autor/a:** Iván Valderrama

**Profesor/a Guía:** María Cecilia Bravo
**Profesor/a Informante:** Patricia Peña

| ASPECTOS A EVALUAR |
|---|
| **1. FORMULACIÓN Y FUNDAMENTACIÓN DEL PROBLEMA** |
| • El problema está planteado de manera precisa y coherente.<br>• La pregunta de investigación se desprende coherentemente de los antecedentes del problema planteados.<br>• Se justifica en forma adecuada la relevancia del problema a investigar y el aporte de la investigación al campo de la comunicación |
| **2. OBJETIVOS** |
| • El objetivo general del proyecto está formulado en forma clara, precisa y coherente, desprendiéndose de la pregunta de investigación.<br>• Los objetivos específicos del proyecto son formulados explícitamente, se detallan los contenidos del objetivo general y se mantiene la coherencia con la pregunta de investigación. |
| **3. MARCO DE REFERENCIA TEÓRICO** |
| • El marco de referencia presenta un conjunto de teorías generales que abordan el problema de investigación.<br>• El marco de referencia presenta un conjunto de antecedentes teórico-empíricos actualizados, directamente vinculados al problema de la investigación.<br>• El marco de referencia se organiza de manera lógica y refleja una elaboración por parte del (a) alumno(a) y no una simple enumeración de teorías. |
| **4. MARCO DE REFERENCIA METODOLÓGICO** |
| • El enfoque metodológico está adecuadamente definido y justificado, es coherente con el problema de investigación y mantiene relación con el logro de los objetivos.<br>• Adecuada definición de los conceptos teóricos y/o variables de la investigación.<br>• El universo y/o el tipo muestral está bien definido, caracterizado, y es coherente con el problema y objetivos de estudio.<br>• Las técnicas de producción de datos se encuentra adecuadamente identificadas y definidas, manteniendo coherencia con el enfoque metodológico.<br>• Las técnicas de análisis de datos, se encuentran definidas y caracterizadas, son adecuadas a los objetivos de la investigación y son pertinentes con el enfoque metodológico.<br>• Se justifica la validez, confiabilidad y/o calidad del diseño metodológico. |

**5. ANÁLISIS Y/0 DISCUSIÓN DE RESULTADOS**

- El análisis de datos presentado está adecuadamente desarrollado y es pertinente a la producción de datos, manteniendo coherencia con los objetivos de la investigación.
- La discusión de los datos se relaciona con el marco de referencia teórico.
- Se utilizan las citas textuales y/o numéricas de los datos en forma integrada al texto de análisis.

**6. CONCLUSIONES, SUGERENCIAS Y PROYECCIONES**

- Las conclusiones reflejan la unidad de todo el proceso de investigación.
- Las conclusiones se presentan en forma clara y coherente con el análisis y los objetivos planteados.
- Las sugerencias se desprenden de las conclusiones y el proceso analítico presentado.
- Presenta sugerencias teóricas, metodológicas y/o prácticas proponiendo nuevas líneas y/o temas de investigación.
- Se indican proyecciones adecuadas y relacionadas con la investigación desarrollada en el contexto del área específica o campo de la comunicación.

**7. BIBLIOGRAFÍA**

- La bibliografía es relevante en cuanto a la calidad de los textos y fuentes seleccionados, y pertinente en relación al problema de investigación y/o al área de especialización.
- Todos los textos o fuentes citados en el desarrollo de la Memoria se encuentran debidamente registrados en la Bibliografía.
- Todas las citas se presentan de acuerdo a alguna de las normas comúnmente aceptadas para trabajos científicos.

**8. ASPECTOS FORMALES**

- El título sintetiza en forma clara y comprensiva el principal propósito de la investigación.
- Se respetan normas gramaticales y ortográficas.
- La redacción es adecuada.
- Presenta índice, siglas, identifica al autor/a y Profesor/a Guía.

# ESCALA PARA CALIFICAR MEMORIA DE GRADO

| | ITEM EVALUADO | PUNTAJES | | | | | | | | multiplicar por | PUNTAJE |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | Formulación y Fundamentación de problema | 1 | 2 | 3 | 4 | 5 | **6** | **7** | 5,8 | 0.10 | **0,58** |
| | | | | | | | | | | | |
| 2 | Objetivos | 1 | 2 | 3 | 4 | 5 | 6 | **7** | 5,5 | 0,05 | **0,275** |
| | | | | | | | | | | | |
| 3 | Marco de Referencia Teórico | 1 | 2 | 3 | 4 | 5 | 6 | **7** | 5,8 | 0.20 | **1,16** |
| | | | | | | | | | | | |
| 4 | Marco de Referencia Metodológico | 1 | 2 | 3 | 4 | 5 | **6** | 7 | 5,5 | 0.15 | **0,825** |
| | | | | | | | | | | | |
| 5 | Resultados (Análisis y Discusión) | 1 | 2 | 3 | 4 | 5 | **6** | 7 | 5,8 | 0.20 | **1,16** |
| | | | | | | | | | | | |
| 6 | Conclusiones | 1 | 2 | 3 | 4 | 5 | **6** | 7 | 5,8 | 0.15 | **0,928** |
| | | | | | | | | | | | |
| 7 | Bibliografía | 1 | 2 | 3 | 4 | 5 | 6 | **7** | 6 | 0.10 | **0,6** |
| | | | | | | | | | | | |
| 8 | Aspectos formales | 1 | 2 | 3 | 4 | 5 | 6 | **7** | 6 | 0.05 | **0,3** |

**5,8**

PTJE FINAL

## INFORME DE EVALUACIÓN

### 1. FORMULACIÓN Y FUNDAMENTACIÓN DEL PROBLEMA

Si bien el estudiante propone un tema clave e importante de estudiar, y efectivamente poco abordados desde los estudios de la comunicación, y eso es lo que se agradece de esta tesis, el problema / tema propuesto es muy amplio y eso hace que tanto la formulación del problema como su operacionalización tampoco ayude a focalizar/acotar lo que se busca evidenciar, explorar, etc: el rol y la construcción de discursos que hace la prensa sobre lo que implica la vigilancia estatal tecnológica/electrónica y el derecho privacidad.
Por ejemplo para el caso: cómo la noticia del uso de software(s) de espionaje de la empresa Hacking Team, con fines de vigilancia – espionaje, son abordados en 2 medios de prensa, en su construcción noticiosa en relación a las implicancias sobre vigilancia estatal de las comunicaciones ciudadanas y el derecho a la privacidad.

### 2. OBJETIVOS

Por lo señalado en el punto 1., los objetivos que se plantea la tesis son también planteados de manera que parecen muy amplis:

a) El objetivo general y los específicos plantean casi 2 investigaciones paralelas- aunque luego se pueda entender que el foco en caso Hacking Team ayude a operacionalizar y acotar el alcance.
-Por ej para el objetivo general hubiera recomendado dejarlo como: abordar la agenda de 2 medios digitales en relación al caso de uso de los softwares de espionaje de Hacking Team en Colombia, en la construcción discurso noticioso sobre vigilancia estatal y privacidad en X período temporal.
-Los objetivos específicos entonces hubieran permitido acotar y operacionalizar: una sistematización sobre cómo se da cuenta o se construye la noticia sobre las implicaciones de la vigilancia estatal en ciudadanos ; y sobre el debate en relación a la privacidad de las comunicaciones de los ciudadanos.

b) A modo de aclaración Cuál es la definición de "prensa escrita digital"? (y porqué se le denomina así) Es importante señalar que la versión online o digital de un medio que existe en prensa escrita, se le considera y denomina a la fecha como medio digital (o sitio web de diario X), ya que en la actualidad las versiones online de un medio escrito tienen 2 características claves: actualización permanente y la posibilidad de la interacción con la "audiencia" (a través de foros, y otros canales de conversación como las redes

sociales de los mismos medios u otros)

**3. MARCO DE REFERENCIA TEÓRICO**

La propuesta de marco de referencia teórico está planteado de manera adecuada en relación a los temas que busca cubrir en general: vigilancia estatal, vigilancia hacia los ciudadanos, privacidad en el contexto de una sociedad digital. También hay un buen contexto del caso de Colombia que permite comprender y situar el alcance sociopolítico -histórico del estudio, particularmente importante para comprender el alcance en relación al proceso de paz.

Como detalle, hubiera sido interesante poder especificar mejor el análisis sobre las implicaciones de la vigilancia de las comunicaciones /espionaje que implican las tecnologías digitales. Esto porque particularmente el software de Hacking Team, es parte de una generación de productos y metodologías que implica llegar a dispositivos personales como lo es un laptop o teléfono móvil de manera más precisa y captando metadatos específicos asociados a ese dispositivo – persona.

También hubiera sido interesante poder explayarse más en entregar o incluir el análisis de los reportes que a la fecha han desarrollado las relatorías para la libertad de expresión (particularmente sobre vigilancia de parte de los Estados a los ciudadanos)de la ONU y la Comisión Interamericana de DDHH que han dado especial énfasis a estas temáticas en América Latina en los últimos años.

**4. MARCO DE REFERENCIA METODOLÓGICO**

Esta es una de las debilidades de la tesis, porque si bien plantea una metodología concreta para la definición de la muestra del corpus de noticias a analizar – a través del uso de proquest - también esto implica limitaciones en el análisis de noticias que son parte de medios digitales – donde la información no es sólo texto, sino que también contenido multimedia, interactivo, en relación con redes sociales etc. Hubiera sido también importante de acotar aspectos como si las informaciones estaban etiquetadas en los sitios webs de los medios con ciertas palabras claves, de manera de tener una continuidad o relación.

Luego se plantea el análisis de contenido y discurso de noticias asociadas al caso, en dos medios digitales, pero no queda claro cómo se realizó el proceso más allá la categorización de la muestra entregada a partir de los resultados de la base de datos: se verificó esto con búsquedas en los sitios de los 2 medios en específico?

Un desafío importante en el estudio de medios digitales usando técnicas como el análisis de discurso /contenido es que deja fuera la riqueza y sentido hipertextual – multimedia que tiene el contenido digital. Esto porque fuerza a hacer el análisis lineal / textual a algo que es mucho más enriquecido, dinámico o interactivo.

Otra observación – a modo de sugerencia es que hay softwares como

| |
|---|
| Nvivo que permiten realizar el análisis cualitativo de páginas web etc |
| **5. ANÁLISIS Y DISCUSIÓN DE RESULTADOS** |
| Esta parte queda confusa para lectura de la tesis, en la decisión que toma el estudiante de plantearla como 4 capítulos separados – hubiera sido mejor dejarlo como un gran capítulo con los subtítulos que se proponen en cada capítulo y que tiene que ver finalmente con los alcances de los temas que se van planteando en el análisis.<br>Finalmente, en el detalle de los análisis y discusión de los resultados de la muestra del corpus noticioso se acota a la información obtenida por el diario El Espectador – como se señala también en las conclusiones, no queda claro en estas secciones si no se encontró nada relacionado en el diario El Tiempo.<br>Luego , también es confusa la decisión de la forma de destacar algunas frases o cuñas de noticias en el análisis no menciona quién dice ese texto destacado: el periodista que redacta la noticia, una fuente citada...? |
| **6. CONCLUSIONES** |
| Las conclusiones sistematizan y dan cuenta del proceso de investigación que se ha mencionado antes, y también del aprendizaje del tesista.<br>Se destaca también la importancia del tema y del caso, en relación a una serie de situaciones que se van a extender por toda América Latina.<br>Para la defensa de la tesis, recomiendo particularmente comentar sobre:<br>- los desafíos que implica realizar investigación en este tema y sus proyecciones<br>- los desafíos metodológicos que tiene investigar sobre el contenido noticioso de medios digitales |
| **7. BIBLIOGRAFÍA** |
| Hay una correcta y actualizada selección de bibliografía |
| **8. ASPECTOS FORMALES** |
| El texto está bien escrito y redactado.<br>Sobre la forma de organizar la tesis, sólo reiterar la observación de que debería haber sólo un capítulo que se llama Análisis y Discusión de los resultados los capítulos IV, V, VI y VII |
| **9. OBSERVACIONES** |
| |

Nombre y Firma:
Patricia Peña Miranda

Fecha: 15 marzo 2017

# PAUTA DE EVALUACIÓN
# MAGISTER EN COMUNICACIÓN SOCIAL

**Título:** Agenda de la prensa escrita digital respecto a los temas de la privacidad de la ciudadanía y la vigilancia estatal en Colombia durante el período 2015-2016: sistemas de vigilancia estatal y el caso Hacking Team.
**Autor/a:** Iván Valderrama Espejo

**Profesor/a Guía:** María Cecilia Bravo
**Profesor/a Informante:** Jorge Iturriaga

| ASPECTOS A EVALUAR |
|---|
| **1. FORMULACIÓN Y FUNDAMENTACIÓN DEL PROBLEMA** |
| • El problema está planteado de manera precisa y coherente.<br>• La pregunta de investigación se desprende coherentemente de los antecedentes del problema planteados.<br>• Se justifica en forma adecuada la relevancia del problema a investigar y el aporte de la investigación al campo de la comunicación |
| **2. OBJETIVOS** |
| • El objetivo general del proyecto está formulado en forma clara, precisa y coherente, desprendiéndose de la pregunta de investigación.<br>• Los objetivos específicos del proyecto son formulados explícitamente, se detallan los contenidos del objetivo general y se mantiene la coherencia con la pregunta de investigación. |
| **3. MARCO DE REFERENCIA TEÓRICO** |
| • El marco de referencia presenta un conjunto de teorías generales que abordan el problema de investigación.<br>• El marco de referencia presenta un conjunto de antecedentes teórico-empíricos actualizados, directamente vinculados al problema de la investigación.<br>• El marco de referencia se organiza de manera lógica y refleja una elaboración por parte del (a) alumno(a) y no una simple enumeración de teorías. |
| **4. MARCO DE REFERENCIA METODOLÓGICO** |
| • El enfoque metodológico está adecuadamente definido y justificado, es coherente con el problema de investigación y mantiene relación con el logro de los objetivos.<br>• Adecuada definición de los conceptos teóricos y/o variables de la investigación.<br>• El universo y/o el tipo muestral está bien definido, caracterizado, y es coherente con el problema y objetivos de estudio.<br>• Las técnicas de producción de datos se encuentran adecuadamente identificadas y definidas, manteniendo coherencia con el enfoque metodológico.<br>• Las técnicas de análisis de datos se encuentran definidas y caracterizadas, son adecuadas a los objetivos de la investigación y son pertinentes con el enfoque metodológico.<br>• Se justifica la validez, confiabilidad y/o calidad del diseño metodológico. |

**5. ANÁLISIS Y/0 DISCUSIÓN DE RESULTADOS**

- El análisis de datos presentado está adecuadamente desarrollado y es pertinente a la producción de datos, manteniendo coherencia con los objetivos de la investigación.
- La discusión de los datos se relaciona con el marco de referencia teórico.
- Se utilizan las citas textuales y/o numéricas de los datos en forma integrada al texto de análisis.

**6. CONCLUSIONES, SUGERENCIAS Y PROYECCIONES**

- Las conclusiones reflejan la unidad de todo el proceso de investigación.
- Las conclusiones se presentan en forma clara y coherente con el análisis y los objetivos planteados.
- Las sugerencias se desprenden de las conclusiones y el proceso analítico presentado.
- Presenta sugerencias teóricas, metodológicas y/o prácticas proponiendo nuevas líneas y/o temas de investigación.
- Se indican proyecciones adecuadas y relacionadas con la investigación desarrollada en el contexto del área específica o campo de la comunicación.

**7. BIBLIOGRAFÍA**

- La bibliografía es relevante en cuanto a la calidad de los textos y fuentes seleccionados, y pertinente en relación al problema de investigación y/o al área de especialización.
- Todos los textos o fuentes citados en el desarrollo de la Memoria se encuentran debidamente registrados en la Bibliografía.
- Todas las citas se presentan de acuerdo a alguna de las normas comúnmente aceptadas para trabajos científicos.

**8. ASPECTOS FORMALES**

- El título sintetiza en forma clara y comprensiva el principal propósito de la investigación.
- Se respetan normas gramaticales y ortográficas.
- La redacción es adecuada.
- Presenta índice, siglas, identifica al autor/a y Profesor/a Guía.

# ESCALA PARA CALIFICAR MEMORIA DE GRADO

| | ITEM EVALUADO | PUNTAJES | | | | | | | | multiplicar por | PUNTAJE |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | Formulación y Fundamentación de problema | 1 | 2 | 3 | 4 | 5 | **6** | **7** | | 0.10 | **6** |
| | | | | | | | | | | | |
| 2 | Objetivos | 1 | 2 | 3 | 4 | 5 | 6 | **7** | | 0,05 | **6** |
| | | | | | | | | | | | |
| 3 | Marco de Referencia Teórico | 1 | 2 | 3 | 4 | 5 | 6 | **7** | | 0.20 | **7** |
| | | | | | | | | | | | |
| 4 | Marco de Referencia Metodológico | 1 | 2 | 3 | 4 | 5 | **6** | 7 | | 0.15 | **5** |
| | | | | | | | | | | | |
| 5 | Resultados (Análisis y Discusión) | 1 | 2 | 3 | 4 | 5 | **6** | 7 | | 0.20 | **5** |
| | | | | | | | | | | | |
| 6 | Conclusiones | 1 | 2 | 3 | 4 | 5 | **6** | 7 | | 0.15 | **5** |
| | | | | | | | | | | | |
| 7 | Bibliografía | 1 | 2 | 3 | 4 | 5 | 6 | **7** | | 0.10 | **7** |
| | | | | | | | | | | | |
| 8 | Aspectos formales | 1 | 2 | 3 | 4 | 5 | 6 | **7** | | 0.05 | **6** |

**5,8**

PTJE FINAL

## INFORME DE EVALUACIÓN

## 1. FORMULACIÓN Y FUNDAMENTACIÓN DEL PROBLEMA

La tesis aborda un problema contingente y de alta relevancia para el campo de las comunicaciones actuales, que es la pregunta por cuan abierta o restringida es la esfera de la comunicación digital en América Latina contemporánea lo que, finalmente, lleva a reflexionar sobre la calidad de nuestras democracias. El problema está bastante bien fundamentado, a partir de la vinculación entre el desarme de las FARC y la vigilancia estatal. Ahora bien, la pregunta da por hecho que existe una agenda por parte de los medios sobre el tema al plantearse "¿Cuál es la agenda de la prensa…?" Quizás la pregunta debió ser ¿existe una agenda? De hecho, en partes del texto el objetivo se plantea así.

## 2. OBJETIVOS

Los objetivos 1 y 2 está claros y se refieren a operaciones concretas que se pueden encontrar posteriormente en el texto. Sin embargo, el tercero aparece como un poco indeterminado ("describir la construcción de la realidad que entrega la prensa") y sin manifestación en el

texto. En mi visión, para determinar en qué medida los medios construyen realidad se debe medir de alguna manera cómo ciertos grupos sociales en la práctica repiten o siguen lo dicho por los medios.

## 3. MARCO DE REFERENCIA TEÓRICO

Las referencias teóricas usadas son sólidas y atingentes para el tema. Las definiciones de privacidad son muy sugerentes.

## 4. MARCO DE REFERENCIA METODOLÓGICO

En general hay un trabajo muy intenso y correcto de recopilación y clasificación de los datos. La secuencia de recogida de información está muy clara y acertada. Sin embargo, no convence la referencia que hace a la etnometodología, pues no aborda en ningún momento a grupos humanos concretos.
Su materia prima fundamental son dos medios escritos masivos y sin embargo no los caracteriza. ¿Por qué esos dos medios? ¿Qué conglomerados están detrás? ¿Han tenido vínculos con gobiernos o empresas de comunicaciones? Eso es fundamental, pues no solo interesa saber qué se habla sino quien lo dice.

## 5. ANÁLISIS Y DISCUSIÓN DE RESULTADOS

El principal punto en contra que tiene la investigación es el uso de la considerable información recopilada. En primer lugar, abusa de las citas. Se espera de todo autor que haga un trabajo de filtrado de los datos para el lector. Este confía en el autor y le delega la capacidad para sintetizar y no ofrecer toda la información recopilada. Las citas no vienen con su autor, es decir no sabemos si es el diario el que habla, un periodista, un columnista invitado, una agencia internacional, etc.
Por otro lado, solo se ofrece la información bruta, no hay un intento muy sistemático por analizar e interpretar la información (lo de las últimas páginas no alcanza), más allá de simplemente ordenarla por palabras clave. Como mapa puede servir, pero se espera más análisis, interpretación, hipótesis, etc.
Hay una confianza desmedida en la sola presencia del recorte y la mención. Pero eso debe ser puesto en un contexto. Son 69 noticias en un medio y 14 en otro. Da la impresión entonces que en el primero el tema vigilancia y privacidad es importante. Sin embargo, para llegar a eso hay que poner esa cifra en relación con el total de noticias o con la cifra de otros temas. Esas 69 pueden constituir muy poco si es un diario que ofrezca variedad de temas y mucho si es un diario menos diverso

## 6. CONCLUSIONES

Los primeros párrafos resultan confusos en cuanto a saber cuál es el lugar que debiera tener la vigilancia; si es necesaria o no, etc.
Por otro lado, se da por hecho que "la ciudadanía es la principal afectada" por las tecnologías de vigilancia estatal, pero el tema de la investigación no era ese (datos, hechos comprobables), sino la cobertura de la prensa.

## 7. BIBLIOGRAFÍA

La bibliografía es bastante completa

## 8. ASPECTOS FORMALES

La investigación no convence, en términos generales, con su concepto de agenda. Creo que

| |
|---|
| utiliza agenda para hablar de cobertura, pues agenda, como yo lo entiendo se refiere a elementos previamente definidos por el grupo editorial, a partir de una reflexión y toma de decisiones, que son evaluados como de mayor importancia que otros. En este caso, el trabajo no se centra en la visión del medio sobre la vigilancia o la política editorial del medio sobre el tema, sino que se centra en las menciones del tema, la cantidad de veces que apareció. |
| **9. OBSERVACIONES** |
| En p. 53 hay un uso incorrecto del concepto positivismo, cuando escribe "posiciones totalmente positivistas respecto a la vigilancia estatal". Lo confunde con favorable, positivo a. |

Nombre y Firma: Jorge Iturriaga

Fecha: 7 marzo 2018