Apoyo de investigación en la línea de Tecnología, Transparencia y Derechos Humanos en la Organización Dejusticia

María Alejandra García Báez

Trabajo de Grado para Optar al Título de Abogada

Director

Jahir Fabián Díaz Hernández

Magíster en Responsabilidad

Universidad Industrial de Santander

Facultad de Ciencias Humanas

Escuela de Derecho y Ciencia Política

Bucaramanga

2023

Dedicatoria

En primer lugar, quisiera dedicar todo mi trabajo, fruto y esfuerzo a Dios. La guía del espíritu santo, la virgen María y mis santos (amigos) Santa Teresita del niño Jesús y San Benito.

A mi familia, mi mamá, mi papá y mi hermana, quienes fueron mi apoyo, mi mayor inspiración y que me siguieron en todo el transcurso de mi carrera, desde el inicio hasta el fin, incluso si estoy en otra ciudad: su amor y apoyo continuo fue lo que me permitió llegar hasta aquí.

A mis amigos, especialmente a Molly, que ha estado conmigo desde siempre.

A Cande por siempre estar dispuesta a apoyarme, alentarme, y ver siempre la solución a los problemas que son complejos.

Y a todas las personas que estuvieron apoyándome en todo momento, estén cerca o lejos, siempre los mantendré presentes: no hubiese logrado nada de esto sin ustedes.

Agradecimientos

Quiero agradecer de nuevo a Dios, y a mi familia por todo el esfuerzo que requirió culminar este trayecto.

Quisiera agradecer profundamente a mis mentores/profesores: Mónica Cortés Falla, María Fernanda Marín y Fabián Díaz Hernández, quienes inspiraron de manera especial mi deseo investigativo en derecho, especialmente al profesor Fabián por ser mi guía y apoyo durante la realización de este proyecto; a él agradezco su perspectiva innovadora que enriquece enormemente todas las aulas de derecho.

Agradezco también a los semilleros de investigación Comuna Quilombo y Semillero de Estudios Interdisciplinares en Derecho y Justicia Constitucional por sembrar mi gusto y ánimo en el camino de la investigación.

Por último, todo mi agradecimiento a la Institución Dejusticia, por recibirme darme la bienvenida en una nueva ciudad, por todo el apoyo recibido en elegir esta rama del derecho, a Mariana Gómez y a los investigadores pertenecientes (o que pertenecieron) a la línea de tecnología, transparencia y DDHH: María Adelaida Ceballos, Christy Crouse y especialmente a mi asesor Daniel Ospina, por su inclusión en todo momento en los espacios en Dejusticia. Definitivamente fue la mejor experiencia que pude tener.

Tabla de Contenido

Pág.

Lista de figuras.

Pág.

Lista de Apéndices.

Ver apéndices adjuntos

Apéndice A. ChatGPT: contextualización y recomendaciones para investigadores en Dejusticia. (Elaborado por Daniel Ospina y María Alejandra García).

Apéndice B. Relatoría de Seminario Acotado sobre el texto el día 15 de mayo de 2023, libro "Nadando en Mar abierto: revisión de buenas prácticas de la fiscalía" (próximo a publicación".

Apéndice C. Índice del Curso en temas de tecnologías digitales y retos para los DDHH.

Apéndice D. Presentación sobre temas del Curso en temas de tecnologías digitales y retos para los DDHH, presentado a la Escuela D, Dejusticia.

Apéndice E. Índice del Archivo Final de la Comisión de la verdad.

Apéndice F. Índice de investigación en Empresas de tecnología y DDHH.

Glosario

Las definiciones que a continuación se desarrollarán pertenecen al ámbito tecnológico.

Algoritmo: un algoritmo es cualquier procedimiento computacional bien definido que parte de un estado inicial y un valor o un conjunto de valores de entrada, a los cuales se les aplica una secuencia de pasos computacionales finitos, produciendo una salida o solución para XXXX. (Cormen et al, 2009)

***Big data*:** la utilización de análisis predictivo u otros determinados métodos avanzados para extraer valor de los datos a partir de su procesamiento, y rara vez para definir a un determinado tamaño de conjunto de datos. (Arimetrics, 2022)

Datos abiertos: son todos aquellos datos primarios o sin procesar, que se encuentran en formatos estándar e interoperables que facilitan su acceso y reutilización, los cuales están bajo la custodia de las entidades públicas o privadas que cumplen con funciones públicas y que son puestos a disposición de cualquier ciudadano, de forma libre y sin restricciones, con el fin de que terceros puedan reutilizarlos y crear servicios derivados de los mismos. (Ley 1712, 2014. Art 6)

EMNB: empresas de tecnología con modelo de negocios basados en datos, es decir Google, Amazon, Facebook, Twitter, entre otros. (Newman et al, 2020)

GAFAM: es el acrónimo utilizado para referirse a Google, Amazon, Facebook (ahora META), Amazon y Microsoft. Conocidos como “Los gigantes del big data”. (Saura, 2022)

Inteligencia Artificial: conocido por sus siglas IA o AI (*artificial intelligence* en inglés), se entiende como la imitación de los procesos cognitivos humanos con la ayuda de “máquinas”

(Chatterjee, 2020). La misma funciona a través de mecanismos de aprendizaje y percepción del medio en el cual sean programados. El mismo concepto tiene ramificaciones y tipos de inteligencia que explican los sistemas utilizados hoy en día en todo el internet, el más común es el utilizado en plataformas por medio de IA de "referenciales".

Data Trust: según el MinTIC, los ***data trust*** son un modelo de gobierno de datos. Se diferencian de los *Data Commons* y los *Data Marketplaces* en que su modelo de gobernanza se basa en un consejo de administración que tiene la responsabilidad de proteger y compartir los datos de forma ética. Propuestos por primera vez por Lilian Edwards en 2004, los *Data Trusts* son un área activa de investigación por parte de múltiples organizaciones de investigación y política de datos. (Edwards, 2004; en MinTIC 2022)

TIC: las Tecnologías de la Información y las Comunicaciones (TIC), son el conjunto de recursos, herramientas, equipos, programas informáticos, aplicaciones, redes y medios; que permiten la compilación, procesamiento, almacenamiento, transmisión de información como: voz, datos, texto, video e imágenes (Art. 6 Ley 1341 de 2009).

Tecnologías emergentes: se definen como las innovaciones científicas que pueden crear una nueva industria o transformar una existente. Incluyen tecnologías discontinuas derivadas de innovaciones radicales, así como tecnologías más evolucionadas formadas a raíz de la convergencia de ramas de investigación antes separadas. (Gregory & Schoemaker; 2001)

Hiperdigitalización: refiere a un fenómeno de avance tecnológico exponencial, el cual ha hecho un impacto en todos los ámbitos del ser humano, se caracteriza por la forma en como la sociedad funciona ahora en torno a las tecnologías de información para funcionar. (Russo, 2021)

Ciudadanía digital: según Claro et al (2021) se define como la capacidad de los ciudadanos (en cualquier parte del mundo) de participar en la sociedad en línea, y hacer uso de la misma no solo

para cuestiones personales, sino acceder a los derechos que conllevan, por ejemplo: libertad de expresión, acceso a la justicia, salud, etc.

Nativos digitales: personas y estudiantes que nacieron en medio de la era tecnología (Gen Z) marcados por dispositivos electrónicos como computadores, videojuegos, celulares, y otros artefactos que hacen que estén familiarizados con el uso de Internet, aplicaciones y redes sociales. (Prensky, 2001)

Internet: internet es una red internacional que reúne una enorme cantidad de información, personas, computadoras y software funcionando e interactuando en forma cooperativa y global. Internet conforma una especie de laberinto virtual que conecta computadoras de todo el mundo a través de diversos medios. Estos medios se presentan en muchas formas: desde cables de red local (varias máquinas conectadas en una oficina o empresa), a cables telefónicos convencionales, digitales y cables de fibra óptica. La transmisión también puede ser vía satélite o a través de servicios como la telefonía celular. Literalmente Internet significa "red de redes". (Universidad Nacional del Sur, 2010)

Ciberespacio: espacio virtual de interacción, que surge como un espacio relacional, su realidad se construye a través del intercambio de información, por lo cual es un “espacio y medio” al mismo tiempo. (Romero, 2004)

Habeas data: es el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos, y los demás derechos, libertades y garantías constitucionales relacionadas con la recolección, tratamiento y circulación de datos personales. (Ley 1266, 2008. Art 1).

Capitalismo de la vigilancia: concepto definido por Zuboff (2020) el cual se entiende como un nuevo orden económico que exige que reclama las experiencias humanas como material “crudo”

y gratis para prácticas comerciales de extracción, predicción y ventas; como concepto primario, sin embargo, también refiere al marco fundacional de la economía de vigilancia, creando un nuevo poder instrumental que da dominancia según las empresas de tecnología (Zuboff, 2020, p. 8)

Sociedad de la información: es aquella en la cual las tecnologías que facilitan la creación, distribución y manipulación de la información juegan un papel importante en las actividades sociales, culturales y económicas debe estar centrada en la persona, integradora y orientada al desarrollo, en que todos puedan crear, consultar, utilizar y compartir la información y el conocimiento, para que las personas, las comunidades y los pueblos puedan emplear plenamente sus posibilidades en la promoción de su desarrollo sostenible y en la mejora de su calidad de vida. (MinTic, 2021)

Disrupción: en el ámbito de tecnologías, es una situación que rompe los esquemas establecidos hasta ahora, entre las cuales se incluyen la inteligencia artificial, robótica, macro datos, blockchain, entre otras. (De la Torre, 2018)

Resumen

Título: Apoyo de Investigación en la Línea de Tecnología, Transparencia y Derechos Humanos en la Organización Dejusticia[*]

Autora: María Alejandra García Baéz[**]

Palabras Clave: tecnologías de la información y la comunicación, datos, vigilancia estatal, derechos humanos, transparencia, acceso a la información.

Descripción:

El presente documento aborda la práctica socio-jurídica en el Centro de Estudios Dejusticia, institución con enfoque principalmente investigativo, por lo cual este trabajo de grado tiene dicho énfasis. Las prácticas se realizaron en la línea de Tecnología, Transparencia y Derechos humanos (una de las varias líneas de investigación en las cuales trabaja Dejusticia), en la cual se abordan diversos temas, siendo los más importantes: acceso a la información, brecha digital, vigilancia estatal, responsabilidad de empresas de tecnología y análisis, impacto y transformación de fenómenos tecnológicos en el siglo XXI. El objetivo principal de este trabajo se delimitó en la investigación de dichos fenómenos, los cuales forman parte de nuestro entorno cotidiano, pero a veces no se comprenden a partir de su ineludible incidencia en el ejercicio de los Derechos Humanos, la cual queda relegada a un segundo plano. En este sentido, la iniciativa de reconocer, estudiar y explicar los efectos de la tecnología en diferentes ámbitos permite que se garantice el respeto pleno de la Constitución Política y se lleven a cabo acciones que busquen el restablecimiento de derechos fundamentales como la dignidad, la privacidad, la libertad de expresión, educación, entre otros.

La visión institucional del centro de estudios Dejusticia, apuesta a la transformación de nuestra sociedad por medio de la investigación y la acción, analizando y participando

[*] Trabajo de Grado

[**] Facultad de Ciencias Humanas. Escuela de Derecho y Ciencias políticas. Derecho y Ciencias políticas. Director: Jahir Fabián Díaz Hernández, Docente Asistente.

de forma activa para lograr una difusión global que logre un impacto positivo en la sociedad.

Abstract

Title: Research Support In The Line Of Technology, Transparency And Human Rights In The Organization Dejusticia*

Author(s): María Alejandra García Baéz[1]

Key Words: technology, state surveillance, human rights, transparency, access to information.

Description:

This document deals with the socio-legal practice at the Dejusticia Center for Studies, an institution with a mainly research focus, which is why this degree work has that emphasis. The practices were carried out in the line of Technology, Transparency and Human Rights (one of the several lines of research in which Dejusticia works), in which various topics are addressed, the most important being: access to information, digital divide, state surveillance, responsibility of technology companies and analysis, impact and transformation of technological phenomena in the 21st century. The main objective of this work was delimited in the investigation of these phenomena, which are part of our daily environment, but sometimes are not understood from its unavoidable impact on the exercise of human rights, which is relegated to the background. In this sense, the initiative to recognize, study and explain the effects of technology in different areas allows to guarantee the full respect of the Political Constitution and to carry out actions that seek the restoration of fundamental rights such as dignity, privacy, freedom of expression, education, among others.

The institutional vision of the Dejusticia it's committed to the transformation of our society through research and action, analyzing and participating actively to achieve a global dissemination that achieves a positive impact on society.

---

* Degree Work

[1]School of Human Sciences. School of Law and Political Science. Law and Political Sciences. Director: Jahir Fabián Díaz Hernández

Introducción

Las tecnologías de la información y la comunicación han generado cambios abruptos y vertiginosos en el desarrollo de los seres humanos y de las comunidades. Particularmente, en el siglo XXI ha derivado – y continúa haciéndolo estrepitosamente – una serie de cuestiones que hacen importante su cuestionamiento, especialmente cuando dicho elemento ha tenido un desarrollo exponencial y permanente en la forma en como percibimos el mundo, haciendo énfasis en la pandemia de la COVID-19.

El imperante avance de las tecnologías y el fenómeno de hiperdigitalización son conceptos que presenciamos en nuestro día y a día. El cuestionarse por el impacto que tienen en nuestras vidas y en nuestros derechos, resulta una cuestión secundaria al goce de lo que nos pueden dar los avances tecnológicos de primera mano.

Fijar la atención en los derechos humanos para incitar a que siempre prevalezcan estos encontrando puntos de equilibrio que los concilien frente a los indudables beneficios al progreso, resulta a veces prescindible y, cuando no, subversivo en un contexto centrado específicamente de las bondades tangibles del desarrollo de las nuevas tecnologías sin reparar en el precio que se paga cuando el horizonte lo marca exclusivamente la lógica del mercado y los negocios. Así pues, los seres humanos han puesto su "atención" – para distraerse – en la forma de analizar el comportamiento humano y recrearlo (IA) de tal forma que olvidaron tener en cuenta las dimensiones personales que cambian por completo, la forma en como pensamos o percibimos el mundo (Schneir, 2015). A su vez la manera en que pensamos o procesamos la información, gracias a la afectación directa por el uso de dichas tecnologías impide pensar/ver el derecho como un ente

aislado a dichas realidades, pues lo contrario, conllevaría la deshumanización (indignidad) y, por contera, la pérdida progresiva de todo el avance que se ha logrado en materia de Derechos Humanos en el último siglo. Tal es el proceso de deshumanización que se habla de personas en términos de datos y se apuesta por aumentar los índices de predictibilidad del comportamiento humano para lograr la uniformidad. Según Weinberger (2019):

> Pero con nuestras nuevas tecnologías, especialmente el *machine learning* y el internet, traen consigo la inmensidad de datos e información que hay alrededor de nosotros, estamos empezando a aceptar la compleja verdad del mundo, mucho más allá de nuestras leyes y modelos concebidos para explicarlo. (p. 8)

Es por ello que el enfoque de esta investigación tuvo como eje principal el impacto de la tecnología en la vulneración de los derechos humanos, por no entender los cambios fenomenológicos de la tecnología, lo que hace que en muchos casos no se perciba dicha conculcación, centrándose específicamente en los derechos de libertad de expresión, privacidad, igualdad, transparencia y buena fe. Continuamente la vulneración de estos derechos debajo del radar de las organizaciones e instituciones que velan por proteger dichos intereses, y más aún en la ubicación de un contexto específico, como corresponde a Colombia.

Según Newman & Ospina (2020):

> Las TIC recolectan y generan datos digitales gracias a internet, las redes sociales, nuestros dispositivos móviles, las aplicaciones que descargamos en ellos, y a muchas otras interacciones digitales que componen el día a día de gran cantidad de personas. Todos estos datos tienen gran valor para quien sepa y pueda analizarlos. (p. 12)

Por lo tanto, es válido cuestionarse no solamente sobre el avance de la tecnología y cómo ahora nos adaptamos a la misma, sino en la información que generan dichos datos digitales: ¿quién

los usa? ¿Qué intereses hay en juego? ¿Son realmente transparentes las herramientas que utilizamos a diario? ¿Hasta qué punto llega mi decisión -libre- de dar mi información? ¿Soy realmente propietario de información y mantengo el control de la misma? Dichas preguntas, tendrán su análisis correspondiente partiendo de la base -y explicación- del sistema conocido como *"Capitalismo de vigilancia",* creado por Zuboff (2020):

> El capitalismo de la vigilancia reclama unilateralmente para sí la experiencia humana, entendiéndola como una materia prima gratuita que puede traducir en datos de comportamiento. (p. 12).

El análisis parte de la investigación por diversos temas, los cuales se abordarán en el desarrollo de este trabajo, siempre teniendo en cuenta la transversalidad de los Derechos Humanos en cada uno de los enfoques presentados: la explicación sobre el capitalismo de vigilancia y la membrana social sobre cómo funcionan las tecnologías más importantes en la actualidad, para así entender la afectación en derechos como la privacidad, la autonomía en la toma de decisiones -las cuales pueden variar desde productos comerciales hasta candidatos presidenciales-, las políticas de moderación de contenidos, la vigilancia ejercida no solo por Empresas de vigilancia particulares, sino por el Estado; finalizando con abordar el concepto de brecha digital, ubicándonos en el contexto colombiano, específicamente.

La metodología utilizada será de análisis cualitativo, pues se partirá de la recopilación de bibliografía utilizada para la profundización en investigaciones sobre los temas específicos, que permitan dar un alcance más entendible del funcionamiento de las tecnologías, contrastando con propuestas de carácter internacional (ONU, Comisión Europea, OEA); como propuestas a nivel Latinoamericano (Corte Interamericana de Derechos Humanos, CEPAL), finalizando con el análisis de normativa vigente al respecto en el ordenamiento Colombiano, al igual que

jurisprudencia de las altas cortes (Corte Constitucional, Corte Suprema de Justicia) teniendo el apoyo de instituciones de investigación especializadas en los temas correspondientes.

Es de vital importancia aclarar que este es solo un análisis de los temas trabajados durante la práctica ejercida en DEJUSTICIA, pues este tema tiene una cantidad considerable de información que sobrepasaría el objeto de explicación de este trabajo de grado.

2. Objetivos

2.1 Objetivo General

Analizar el impacto de los usos de las TIC en los Derechos Humanos desde la línea de Tecnología, Transparencia y Derechos humanos en la Institución Dejusticia.

2.2 Objetivos Específicos

Revisar de forma sistemática y activa bibliografía propuesta en el marco de la práctica, concerniente a los temas de tecnología y derechos humanos, acceso a datos, brecha digital y ecología.

Organizar los temas más imperantes trabajados durante la práctica y su afectación en los Derechos humanos.

Interpretar las investigaciones realizadas en la línea de tecnología, transparencia y derechos humanos para así poder mostrar avances en sus resultados.

Destacar la importancia de la comprensión de los usos de las TIC para que siempre se enmarquen en el respeto de la Constitución Política y el catálogo de derechos humanos.

3. Información sobre la Institución Dejusticia

3.1.Misión

Dejusticia es un centro de estudios jurídicos y sociales localizado en Bogotá, Colombia. Su misión principal se dedica al fortalecimiento del Estado de Derecho y a la promoción de los derechos humanos en Colombia y en el Sur Global. Promueve el cambio social a través de estudios rigurosos y sólidas propuestas de políticas públicas, y adelanta campañas de incidencia en foros de alto impacto. También lleva a cabo litigios estratégicos y diseña e impartimos programas educativos y de formación.

3.2.Visión y teoría de cambio

La institución Dejusticia corresponde al modelo de un centro de investigación-acción, en el cual se promueve la concepción de ciudadanía incluyente, es decir, una sociedad en la que sus ciudadanos se sientan incluidos y a la vez sean incluyentes; se sientan empoderados para reclamar sus derechos frente a unas instituciones que los garanticen efectivamente; unos ciudadanos que entiendan y se comprometan con el ideal de una democracia incluyente y reclamen del Estado y de todas las instituciones que los afecten, los mismos ideales.

Su objeto social se circunscribe a impulsar el cambio y promover estos círculos virtuosos, usando la experticia propia de institución en temas que afectan a la población colombiana, para ampliar, enriquecer y apoyar las acciones de individuos y comunidades en los reclamos de sus derechos; aumentar y democratizar el acceso a la formación en derechos humanos y estrategias de acción de las comunidades, los activistas y los investigadores y finalmente haciendo propuestas

concretas para mejorar las instituciones para que estas sean capaces de proteger y garantizar los derechos de los ciudadanos. (Dejusticia, 2020)

3.3.Reseña histórica

Dejusticia fue fundada en 2005 en Bogotá, Colombia por el escritor y columnista colombiano Mauricio García Villegas, la abogada y profesora colombiana Helena Alviar García, el profesor y jurista colombiano Rodrigo Uprimny, el profesor universitario César Rodríguez Garavito, la abogada y profesora colombiana Catalina Botero y los académicos Juan Fernando Jaramillo, Danilo Rojas y Diego E. López Medina. La organización consolidó su Editorial Dejusticia en 2009 y en 2016 su área de Litigio bajo la Dirección General de Rodrigo Uprimny.

La organización crea y proporciona documentos académicos e informes a nivel mundial contra la injusticia, la desigualdad, los derechos humanos y otros diversos problemas sociales. Y también ayuda a las comunidades marginadas a través de los esfuerzos en litigio. (KAS, 2018)

Dejusticia también organiza encuentros internacionales y produce documentos de trabajo para promover el debate sobre las ideas que apoyan los derechos humanos, el Estado de Derecho, la cultura jurídica y la crisis de la justicia.

3.4.Áreas de investigación

Las áreas conformadas dentro de la organización competen a una línea de investigación específica, a saber: Área de Género; Área Internacional; Área de Litigio, Comunicaciones, Coordinación de proyectos; Editorial Dejusticia; Escuela D; Línea Étnica Racial; Línea Justicia Ambiental; Línea Justicia Económica; Justicia Fiscal; Línea Justicia Transicional; Línea Política de Drogas; Línea Sistema Judicial; Línea de Tecnología, Transparencia y Derechos Humanos; Línea Tierras y Campesinado. Cada una de estas líneas lleva a cabo investigación e incidencia, abordando los contextos políticos y legales relevantes. Trabajan a nivel nacional (en Colombia) e

internacional a través de colaboraciones con aliados en el sur y norte global, y a través de acciones directas y participación en foros internacionales de derechos humanos.

3.5.Línea de Tecnología, Transparencia y Derechos Humanos.

El área específica en la cual se ejerció la práctica es la línea **de TECNOLOGÍA, TRANSPARENCIA Y DERECHOS HUMANOS**, cuya coordinadora actual es María Adelaida Ceballos. Las investigaciones se pueden llevar a cabo en conjunto con investigadores asociados (*fellows*) o de carácter interno; el investigador titular en temas de Tecnología, Transparencia y acceso a la información corresponde a Daniel Ospina-Celis, quien fue el asesor asignado durante la práctica.

Los temas generales trabajados en la línea corresponden a: el acceso a la información pública como condición básica de la democracia y el impacto de la tecnología en los derechos humanos, especialmente en una sociedad desigual, a su vez, trabajando de manera conjunta con la misión y enfoque de la institución. La pregunta que debe atravesar la creación de todos los proyectos es el impacto o vulneración de algún Derecho Humano o Derecho fundamental.

De igual manera, se intentan entender los distintos fenómenos tecnológicos por medio de la investigación y puesta en conocimiento pública o interna de columnas, libros, reseñas, ponencias o artículos académicos. Esto, para que todos los actores cuenten con la información de calidad que permita la toma de decisiones razonables. Algunos de los temas abordados durante la práctica correspondieron a:

- **Inteligencia artificial:**

  Investigación breve sobre ChatGPT, documento que sirve de base para responder preguntas básicas sobre su funcionamiento y confiabilidad en respuesta, así como una lista de

recursos para investigadores e impactos en los DDHH.[2] De esta manera, se sigue la investigación que por presunto indebido tratamiento de datos personales a iniciado la Superintendencia de Industria y Comercio contra CHATGPT. El mismo se difundió en la institución Dejusticia (por medio del correo electrónico) el día lunes 15 de mayo y se adjuntará en los anexos correspondientes, la autoría corresponde a Daniel Ospina (asesor) y María Alejandra García.

- **Fiscalía General de la Nación y la investigación de la corrupción: obstáculos y buenas prácticas.**

El tema de transparencia de funcionarios públicos conforma uno de los puntos principales de la línea, en el cual se apoyó desde la moderación y comentarios correspondientes a la investigación hecha en conjunto con la línea de Sistema Judicial, sobre la investigación de casos de corrupción y delitos relacionados con el abuso de función pública, concusión, contrato sin cumplimiento de requisitos legales, corrupción privada, celebración indebida de contratos, utilización indebida de información e influencias y el abuso de autoridad durante los últimos 5 años; concluyendo con el análisis de sus buenas prácticas y obstáculos dados por la misma institución al investigar este tipo de delitos[3]. El libro tiene por título: "*Nadar en mar abierto: Obstáculos y buenas prácticas de la Fiscalía General de la Nación en la investigación de la corrupción"* (el cual está próximo a publicación). Se trabajó en la relatoría del Seminario Acotado

[2] El texto será puesto en anexos correspondientes pues fue de difusión interna en la Dejusticia.

[3] No se puede desplegar información específica sobre esta investigación pues aún está en proceso de publicación. Sin embargo, todas las publicaciones de Dejusticia son de acceso público, por el cual se espera que el mismo se pueda evidenciar en un futuro cercano.

sobre el texto el día 15 de mayo de 2023, anotando todos los comentarios para su contextualización y agregación al texto para los escritos (relatoría adjunta en anexos); por otro lado, durante la semana del 22-30 de mayo se trabajó en la edición del texto y las referencias bibliográficas en conjunto con la investigadora Christy Crouse.

- **Propuestas de investigación: Acuerdo de Escazú y Mercado de Bonos de Carbono.**

Cada año, en la Institución se elige un tema que deben abordar todas las líneas de forma transversal. El tema del año 2023 concierne al Cambio Climático y la defensa de derechos humanos conexos al mismo. En el marco de la línea se trabajó principalmente el aspecto de transparencia, tanto del Gobierno como de Empresas Privadas, respecto a cifras concernientes al Mercado de Bonos de Carbono y la implementación correcta del Acuerdo de Escazú; específicamente en lo que afecta al acceso de información medioambiental, y cómo el mismo garantiza un medio ambiente sano. Para ello se trabajó durante todo el mes de mayo y la primera semana de junio en la sistematización de referencias bibliográficas para entender el contexto de mercados de carbono, en su ámbito internacional y nacional. Se deja adjunta la sistematización de referencias trabajadas en conjunto con la investigadora María Adelaida Ceballos.

- **Curso en tecnología e impactos a derechos humanos:**

Dejusticia organiza cursos y talleres para capacitar activistas, líderes de comunidades y profesionales jóvenes de múltiples disciplinas quienes, sin importar su formación inicial, están interesados en desarrollar nuevas opciones de carreras y en obtener las herramientas necesarias para proteger los derechos de sectores vulnerables. Con ello se contribuye a crear y mantener una comunidad del Sur Global que está constantemente nutrida por el trabajo hecho por la institución

y el trabajo de los estudiantes que pasan por sus programas, quienes representan una voz del Sur Global sólida, bien informada y con trayectoria.

Este curso se estructuró con base en la contextualización en general de la comunidad sobre temas de TIC y su afectación en los derechos humanos, consistente en dos sesiones, preparadas en torno a temas como la libertad de expresión en redes sociales, moderación de contenido y uso, algoritmos y discriminación étnico racial, vigilancia estatal y brecha digital. La participación durante el curso consistió en la preparación y estudio de los temas (y subtemas) asociados a las dos sesiones; colaborando también con las relatorías correspondientes de los eventos que después serán de utilidad para trabajos de investigación futuros en la Institución. Las sesiones se dan con invitados expertos en el tema a tratar, aportando a contenidos que permiten una mayor aproximación con los temas, buscando siempre que las demás áreas se nutran de estos temas y con base en ellos se puedan tratar distintos problemas desde otros ángulos en trabajo conjunto del equipo. Es válido aclarar que el curso se dará en el mes de agosto del año en curso, mes en el cual ya no se tendrá práctica vigente con la institución, pero el índice y presentación (entregados en el mes de mayo) se dejará en los anexos correspondientes.

- **Empresas de Tecnología y su responsabilidad frente a los DDHH[4].**

Por su parte, se dio la recopilación y creación de un índice informativo sobre empresas de tecnología durante el mes de abril, y sus afectaciones a derechos humanos en diversos aspectos:

[4] Su difusión no está permitida, sin embargo, se dejan los temas trabajados en el mismo, en caso de que en un futuro se llegue a realizar alguna investigación correspondiente, además de las ya hechas por dejusticia en temas como: brecha digital, vigilancia estatal y responsabilidad de intermediarios y GAFAM frente a manejo de datos.

libertad de expresión, decisión, privacidad, educación; que moldeará investigaciones futuras en caso de que se llegue a hacer una propuesta de investigación en este aspecto.

Los temas fueron:

- *Explicación sobre el avance tecnológico*: cuáles son las empresas de tecnología y sus exponentes más representativos (Google, Amazon, Meta, Apple, Microsoft), y Empresas de tecnología y su forma de operación.
- *Concepto de debida diligencia y discusión sobre uso ("end-use"):* parámetros básicos dados por las Naciones Unidas y la Responsabilidad de las empresas que proveen servicios de tecnología y el uso del mismo por terceros.
- *Responsabilidad de las empresas que proveen servicios de tecnología y el uso del mismo por terceros:* Redes sociales, su intención inicial y su manejo hoy en día. Moderación de contenido, la Preocupación por la privacidad en torno a la afectación del libre albedrío y autonomía en la toma de decisiones.
- *Preocupación por la privacidad en torno a la afectación del libre albedrío y autonomía en la toma de decisiones:* Difusión de información parcializada, Discurso de odio y manejo del mismo en las redes sociales y casos de discursos de odio en las redes sociales.
- *Empresas de servicios en la nube y medio ambiente*: Impacto ambiental de las empresas de almacenamiento en la nube, gasto de energía, emisiones de CO2 y afectación del medioambiente: cuál es su afectación principal.
- *Empresas de servicios de vigilancia y privacidad*: Venta de información al Estado por parte de empresas de vigilancia (*backdoor* y recolección de información por medio de redes sociales), uso de tecnología intrusiva y de reconocimiento facial, y las prácticas de inteligencia estatal – vigilancia.

Este índice fue construido para investigaciones en un futuro en Dejusticia y se dejará como anexo del mismo. El trabajo estuvo dirigido a almacenar información correspondiente a fenómenos tecnológicos, que servirán en un futuro en la línea de investigación de Tecnología. Su difusión fue interna en la línea en el mes de abril y se deja como un documento DRIVE para su fácil acceso a los demás investigadores interesados en el tema.

La participación dada en seminarios y simposios se dio con la intención de retroalimentación interna en temas diversos como:

- **Plan Nacional de Desarrollo (10 de marzo de 2023):** reunión interlíneas para discutir sobre el trabajo conjunto que Dejusticia puede adelantar en el tema de paz total, con la participación de personas muy cercanas a la casa: José Espinosa, Javier Revelo y Nicolás Torres. En tal espacio se dio una conversación interna y preliminar sobre los retos de la paz total desde dos perspectivas: la presencia dispar del Estado en el territorio y las discusiones actuales sobre el Plan Nacional de Desarrollo. Del mismo se elaboró una relatoría que recolectó los comentarios principales dados durante la discusión para la elaboración de un documento de difusión externo, el cual se anexará de forma correspondiente.
- **Seminario Interno - Redes Sociales y Debate Democrático (24 de marzo de 2023):** En este seminario se trató el tema de Cultura de la cancelación en redes sociales. Se participó desde la línea en la anotación de comentarios y retroalimentación al texto en general. No se puede difundir el texto pues está en edición, pero pronto se espera su acceso público.
- **Seminario de discusión: emergencia climática y justicia ambiental (12 de mayo):** Este seminario hace parte de los esfuerzos por desarrollar conceptos y aproximaciones comunes para abordar el tema articulador del año en Dejusticia: Emergencia Climática y Justicia

Ambiental. En este primer seminario se discutió el texto preparado por Sergio Chaparro (Coordinador de la Línea en Derecho Internacional) en torno a las distintas narrativas que existen en torno a la lucha contra el Cambio Climático. La participación del mismo fue presencial y se dieron aportes teniendo como base las investigaciones sobre Empresas de tecnología referenciadas anteriormente.

- **Socialización del proceso de transferencia de la información recolectada por la Comisión de la Verdad a la Jurisdicción Especial para la Paz y el Archivo General de la Nación (17 de marzo):** Esta socialización se dio en el Archivo General de la Nación (Cra 6, #6-91) por parte de la comisión de la verdad en liquidación, sobre los procesos de recolección de documentación y también sobre cómo se guardan en el archivo, liderado por Mauricio Katz (Liquidador de la Comisión de la verdad) y la doctora Ivonne Suárez (directora del AGN). A este evento asistí en representación de Dejusticia para verificar los procedimientos que estaba efectuando la Comisión en el tema de acceso a los documentos y memorias de la comisión de la verdad, pues en este proceso participó la línea de Tecnología, Transparencia y Derechos Humanos. En la misma se hicieron preguntas sobre verificación del índice y su información, con la protección de DDHH. Del mismo se hablará en el texto más adelante. La comisión de la verdad hizo entrega de las memorias el día 26 de mayo de 2023, evento del cual hay registro videográfico. (Comisión de la verdad, 2023)

En su mayoría los elementos de investigación (plataformas como JSTOR; OXFORD library, REPOSITORIO DEJUSTICIA) utilizados dentro de la práctica se proveen por la organización, en temas de textos de investigación, libros, artículos. La institución cuenta con herramientas como correo electrónico personalizado y plataformas (PODIO) para la crítica

colectiva de Columnas o Investigaciones de mayor rango entre los miembros de la misma, donde se busca una participación activa en los espacios para una debida retroalimentación. Los seminarios, reuniones y eventos se dan dentro del recinto - ubicado en la Calle 35 #24-31; que funciona como sede de Dejusticia - si son organizados por la Institución. Por su parte, también se desarrollaron eventos externos apoyados por Dejusticia en el marco de la construcción de alianzas y trabajo cooperativo para alcanzar un impacto mayor.

4. Contexto tecnológico

4.1.Tecnología y su evolución en el siglo XXI

La evolución de las TIC se ha logrado ha surtido un proceso exponencial, especialmente desde finales del siglo XX y principios del siglo XXI. El avance obedeció, en principio, a caracteres donde se buscaba la mayor conectividad, creando así una globalización en las telecomunicaciones modernas, según Rueda (2007):

> En inglés Internet se llama “El Internet”, como si fuera La Red, pero en realidad se trata de centenares de redes interconectadas en todo el mundo, las cuales funcionan mediante la utilización de los mismos protocolos de comunicación. Es por este tipo de interconexión a escala mundial que se puede hablar de Internet como un medio de comunicación social, ya que constituye un medio masivo de comunicación que llega a centenares de personas en un mismo momento y constantemente. Además, se puede considerar, también, como un medio de comunicación interpersonal, ya que constituye una forma de comunicación propia de la relación entre individuos que se desarrolla actualmente. (p. 6)

Por otro lado, el fenómeno de implosión en la *hiperconectividad* data de inicios de 2010 (Rogers, 2022). Esto implica que las plataformas de tecnología como Facebook, Youtube, y

Google cobrasen una relevancia que no solo permitió que millones de personas pudiesen conectarse a un sinfín de posibilidades, sino que cambió la forma en cómo funciona el mundo. Según Carr (2008) “la tecnología no es neutral, cambia las normas sociales e influye en nuestras elecciones” (p.39); especialmente si se tiene en cuenta la relevancia que tienen hoy en día el uso de tecnologías y plataformas, que hace casi imposible que una persona esté por fuera del radar de las mismas (Schneir, 2015). En consonancia con lo anterior Asís (2015) advierte sobre la “capacidad de concentrar el poder político, y de crear nuevas formas de ofuscación y dominación de la sociedad” (p. 25).

Figura 1.

Las cuatro revoluciones industriales.

Nota: Gráfico histórico de las revoluciones industriales, siendo la actual la “cuarta revolución industrial”. Tomado de “Inteligencia Artificial” p. 65. Por Nuria, 2020.

El proceso de hiperdigitalización es denominado comúnmente como “la cuarta revolución industrial”, caracterizado por la utilización de sistemas híbridos de producción, con integración de

datos y conocimientos, creando una centralización en la satisfacción de necesidades individuales de los usuarios o clientes (Newman et al, 2020), y en especial en los datos -uso de datos-, los cuales generamos en una base diaria, gracias al uso de redes sociales, dispositivos móviles, aplicaciones, e interacciones digitales que ejercemos todo el tiempo. Todo esto se da a pesar de que ignoramos las repercusiones que conlleva usarlas. Las EMND (Empresas con modelo en manejo de datos) saben analizarlos y explotarlos en función comercial, es por ello que el concepto de datos es tan importante en el análisis de estas herramientas tecnológicas. Según Upegui y Ospina (2022):

> Las TIC recolectan y generan datos digitales gracias a internet, las redes sociales, nuestros dispositivos móviles, las aplicaciones que descargamos en ellos, y a muchas otras interacciones digitales que componen el día a día de gran cantidad de personas. Todos estos datos tienen gran valor para quien sepa y pueda analizarlos. (p. 12)

Cuando mencionamos el fenómeno tecnológico y su evolución drástica, es de suma importancia mencionar el papel central que juegan Google, Amazon, Meta, Apple y Microsoft (GAFAM), siendo las grandes empresas de internet las que pueden facilitar la creación e investigación del avance de nuevas herramientas con las cuales conviviremos diariamente, y que claramente alteran de forma significativa el orden mundial (Newman, et al, 2020)

Las TIC cumplen un papel determinante en la producción y en el desarrollo social, teniendo en cuenta que el carácter de las mismas se da de manera transversal a la sociedad, caracterizados por su ubicuidad, es decir, su capacidad de estar presente en todas partes y al mismo tiempo.

4.2.Plataformas de tecnología y recolección de datos

El entendimiento de las plataformas tecnológicas se debe analizar desde constructos culturales y socioeconómicos. El uso de plataformas tiene un intricado sistema de procesamiento de datos de manera permanente, a través de algoritmos y protocolos formales, de tal forma que su

producto sea traducido en lo que se aproxime más a la forma deseada por el cliente (Van Dijck, 2013). Por ejemplo, una plataforma como Google está estructurada por un diseño lógico que genera un programa arquitectural, computacional y político, que incluye estrategias de organización de nosotros -los usuarios- y que funcionan de forma estratégica en la recolección de dichos datos (Evans & Schmalensee, 2011).

Su forma de operación parte de la base de la recolección de datos, las fuentes de aquellos datos son proporcionados en gran parte por el usuario o cliente, con la creación de cuentas o perfiles; también por su historial de compras o contenido que consume o sube en cualquier plataforma o aplicación. Así, puede que parte de la información que consignamos para crear un perfil incluya datos sensibles, como ideología política, origen étnico, orientación sexual, intereses, hobbies (Ángel & Newman, 2019). Por otro lado, otra fuente significativa de recolección de datos se da a través de "*web tracking*", el uso de *cookies*[5] o política de tratamiento de datos, a su vez el historial de las cosas que averiguamos en toda nuestra interacción con la internet, incluyendo datos personales como nuestra ubicación geo-espacial en tiempo real, según Scheier (2015):

> Existe toda una industria dedicada a rastrear en tiempo real. Las compañías usan tu teléfono para rastrear en supermercados o tiendas, para aprender como compras; te rastrean en el camino para determinar qué tan cerca estás a alguna tienda en particular, y envían publicidad a tu teléfono basado en dónde estás en este momento. Los datos de locación son

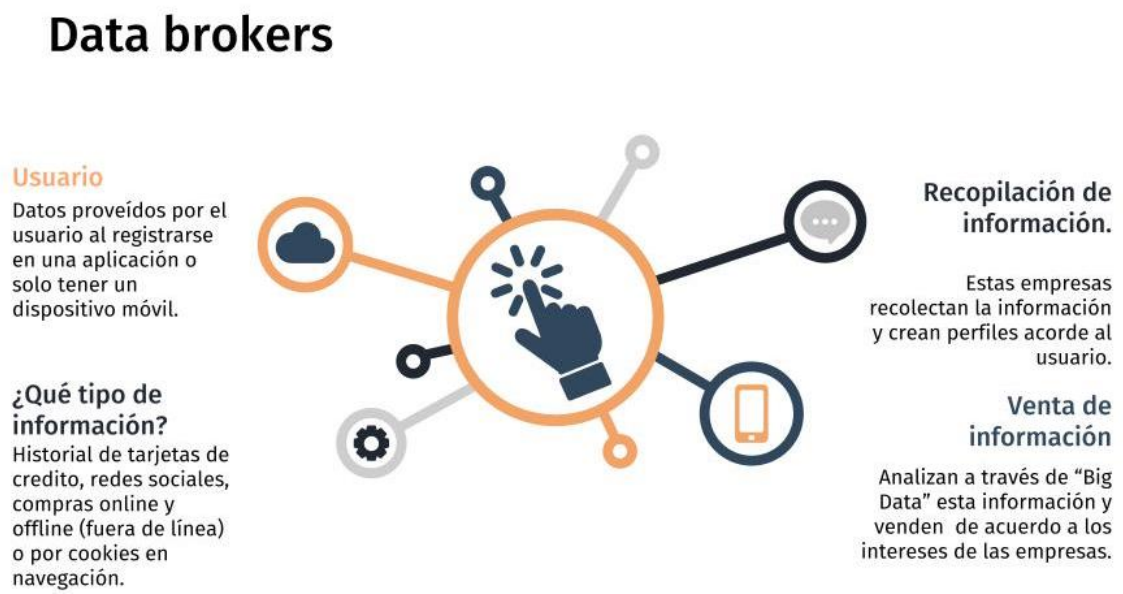
[5] Según Luján (2012): "Una cookie es un paquete de datos que un navegador web almacena de forma automática en el ordenador de un usuario cuando éste visita una página web. La cookie es enviada desde el servidor al visitante de la página web. Posteriormente, cada vez que el usuario visite esa misma página web o alguna otra del mismo dominio, la cookie será leída por el navegador web, sin ser modificada, y devuelta al servidor web".

tan valuables que las compañías de teléfonos están vendiéndolo a *"data brokers"*[6] que venderán esta información a cualquiera que este dispuesto a pagar por ella" (p. 8)

Esta información proveída por terceros corresponde a una alianza estratégica de compañías que pueden prestar servicios a nombre de la empresa, empresas de publicidad o marketing, dedicadas exclusivamente a la recolección de datos, como se evidencia en el siguiente gráfico.

Figura 2.

Funcionamiento de data brokers.



Nota: Explicación sobre el funcionamiento de los data brokers, las empresas más conocidas operan en Estados Unidos, la información que se obtiene sobre las mismas es muy limitada por su forma de operación e intrusión de la privacidad. Adaptado de Lisa (2022). https://www.lisainstitute.com/.

[6] Los data brokers son empresas que recopilan datos de la vida real y virtual de las personas desde diferentes fuentes de datos para venderla a terceras empresas con fines lucrativos. (INCIBE, mayo de 2022)

La recopilación de información y su análisis se da de manera uniforme, encaminado a segmentar y clasificar a los usuarios de acuerdo con sus gustos, preferencias o intereses, para mejorar la experiencia del usuario cuando navegue por la red. No obstante, el excedente conductual de información (Zuboff, 2020), es tratado con fines mercantiles para perfilar a las personas, ofrecerles experiencias personalizadas e influir en la toma de decisiones, v. gr., para la compra de productos y servicios promocionados por las empresas de tecnología. Esta información no es clara. Asimismo, se encuentra que en las políticas de privacidad de las aplicaciones, entre las finalidades de tratamiento de datos personales, pueden mencionarse algunas como prestar un buen servicio, dar descuentos u ofertas, hacer estudios e investigaciones, ofrecer contenido personalizado, y compartir información con terceros, por ejemplo WhatsApp, que comparte información a su vez con Facebook, todo se relaciona, finalmente, a GAFAM (Google, Amazon, Facebook, Apple, Microsoft), según Revilla (2020):

> La clave de la consolidación del llamado imperio GAFAM (Google, Apple, Facebook, Amazon, Microsoft) como superpotencias reside en la cantidad de datos que poseen. Tal es así que estas compañías tienen los perfiles virtuales de sus millones de clientes, una vía de comunicación con estos y otros datos adicionales como pueden ser sus intereses, hábitos o localización, cuentan con ventajas tecnológicas potentes, una sólida capacidad financiera y el capital humano imprescindible para que sus plataformas evolucionen. (p. 16)

Es válido afirmar que tener una cuenta activa en Gmail o Outlook se convirtió en un prerrequisito para el registro de uso de páginas o aplicaciones, o en su defecto una cuenta de Facebook, Instagram o WhatsApp. (Arango, et al. 2020). Bajo este escenario es que se ha considerado que no existen productos y servicios gratuitos, porque el pago se da con nuestros datos

personales e información. En este sentido, los datos personales hoy son considerados el nuevo petróleo.

A pesar de que la visión inicial de GAFAM fuese el "*organizar la información del mundo*" y enriquecer su accesibilidad y utilidad, el modo y funcionamiento de estas tecnologías conllevan la vulneración sistemática de derechos humanos, y es aquí donde surge el concepto planteado por Zuboff (2020), conocido como "*capitalismo de vigilancia*".

4.3.Capitalismo de vigilancia

Este ha sido el análisis más complejo con respecto a la penetración de las TIC en nuestra vida actual y futura, pues su avance y funcionamiento no puede dejar de lado el origen de la sociedad que hasta hace poco conocemos. Es por lo tanto que Google, con su invención de publicidad dirigida y tratamiento de datos, apelando a la idea de conectividad, el internet gira en función de los intereses y creación de dichas empresas, forjando expresiones y posicionando a los datos como "el petróleo del siglo XXI". Normalmente cuando se hace referencia al fenómeno tecnológico, se deja de lado que la concepción fue creada por seres humanos, con ideales y comportamientos específicos, ya que todo lo que parecemos conocer no surge de ninguna fuerza invisible y fue deliberada y construida en puntos históricos específicos. (Zuboff, 2020, p. 94)

Es por lo tanto que, a la cabeza de estas empresas, los avances tecnológicos de inteligencia artificial, algoritmos, y máquinas que mejoren cada día en experiencias nuevas de seres humanos, que luego van a nutrir de información para así replicar en un círculo de intereses particulares.

Según Zuboff (2020):

> Ya no somos los *sujetos* de la realización de valor. Tampoco somos, como algunas voces han insistido en afirmar, el «producto» de las ventas de Google. Somos, más bien, los *objetos* de los que se extrae una materia prima que Google expropia para su uso en sus

> fábricas de predicciones. Las predicciones sobre nuestros comportamientos son los productos de Google y la compañía las vende a sus clientes reales, pero no a nosotros. *Nosotros somos el medio usado al servicio de los fines de otros.*[7] (p. 103)

El hecho de que se permitan avanzar de forma sistemática obedece a la cercanía que cada vez ofrecen a los usuarios, haciendo una especie de "metamorfosis" en los productos que compramos o usamos, como *weareables*[8], drones, sensores, e Inteligencia Artificial, concepto que ha causado bastante revuelo en los últimos años y el fenómeno que normalmente asociamos como el avance sorprendente de la tecnología.

4.4.Aproximación a la Inteligencia Artificial

La inteligencia artificial ha estado presente en la humanidad desde el año 1950, con una prueba ejercida por Alan Turing, en el cual se interaccionó vía texto con un sistema al que se puede hacer preguntas. Si no se logra discernir cuando la respuesta es dada por un humano, entonces la máquina es inteligente. Ejercicios parecidos son los que experimentan aún los ingenieros y programadores en la creación de IA que cada vez se asemejen más al pensamiento humano. Para entender la forma en que funcionan las Inteligencias Artificiales, se debe pensar que las mismas están basadas en las redes neuronales que componen el cerebro humano. La forma en que aprendemos, pensamos o almacenamos información se da por estas redes neuronales y el aprendizaje que tengamos de elementos externos. En contraste a ello, las máquinas tienen también

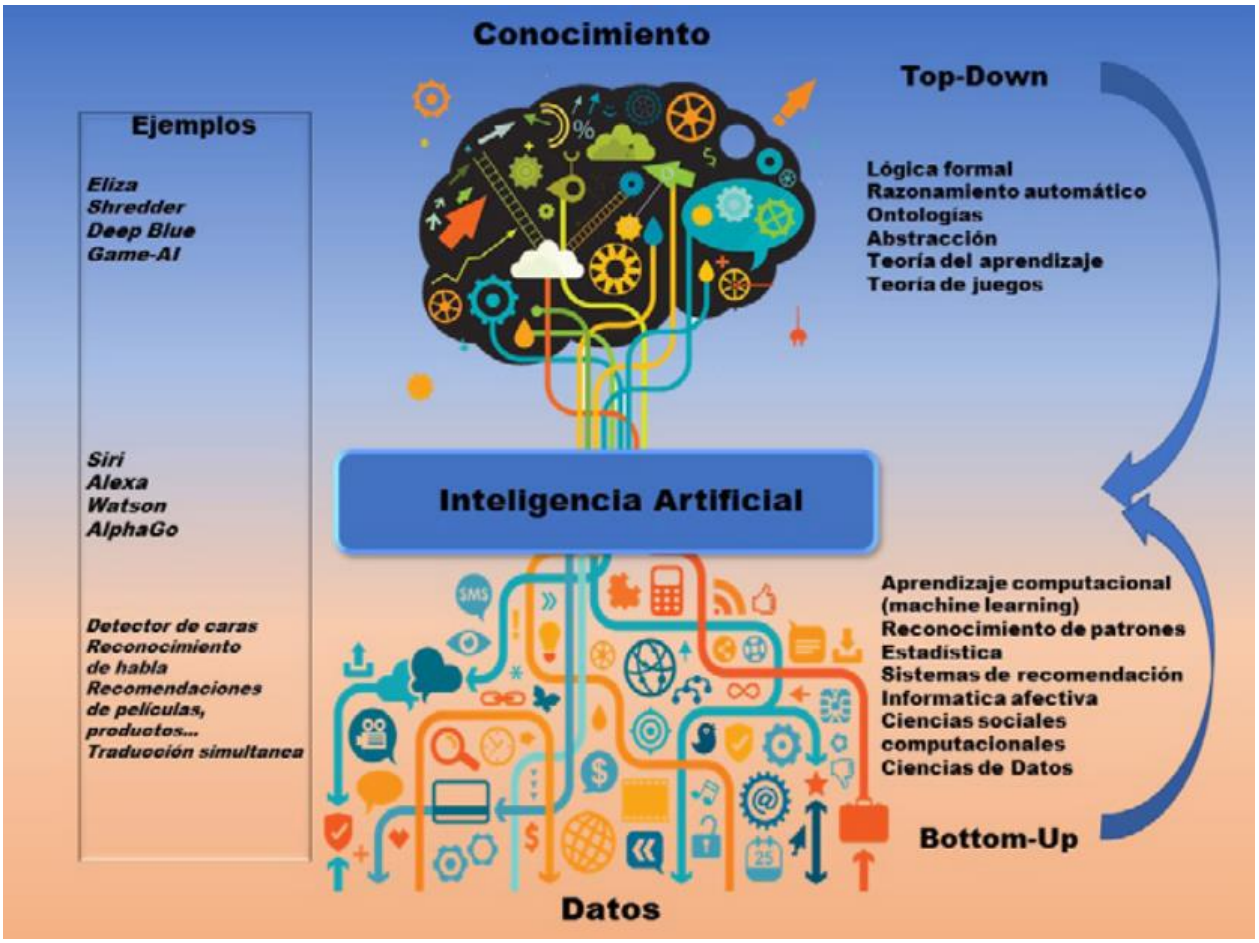
[7] Subrayas originales del texto.

[8] Un wearable es un dispositivo electrónico que se usa en el cuerpo humano y que interactúa con otros aparatos para transmitir o recoger algún tipo de datos. El ejemplo más claro y más conocido de wearable lo constituyen los relojes inteligentes y las pulseras de actividad. (Aritmetics, 2022)

redes neuronales que emulan el modo en que el cerebro humano procesa la información, haciendo un ejercicio simultáneo de capas de información. Por lo tanto, su aprendizaje se puede dar por medio de información programada en ellas o por la interacción con personas, para así ir enriqueciendo su base de datos e información. Este proceso tiene diferentes clasificaciones, dependiendo del volumen de información que manejen; la clasificación más estandarizada corresponde a los modelos de *Machine Learning*, los cuales consisten en los estudios científicos de algoritmos y modelos estadísticos que los modelos de computación usan para hacer tareas específicas sin ser previamente programados de forma explícita para ello (Mahesh, 2019). Por otro lado, una de las ramas más utilizadas en AI corresponde al *Deep learning*, que consiste en una red de tecnología que intenta simular las redes neurales del celebro, permitiendo que aprenda de una gran cantidad de datos, para así dar predicciones a las preguntas, o redactar textos de forma automática (Centeno, 2019). Estos dos modelos componen la mayoría de AI's en la actualidad, siendo ChatGPT un buen ejemplo de ello. (Forero, 2023)

Figura 3.

Ejemplos de sistemas de Inteligencia artificial y su forma de aprendizaje.



Nota: En el gráfico se hace un contraste del cerebro con la inteligencia artificial, en primer lugar, tenemos la forma en que recolectamos información: lógica, razonamiento, abstracción, teoría del aprendizaje, teoría de juegos; en contraste a los métodos de aprendizaje de AI. A su vez algunos ejemplos de cada método de aprendizaje, como Game AI, Siri o Alexa. Adaptado de "Inteligencia Artificial" (Nuria, 2020). https://www.ontsi.es/sites/ontsi/files/2020-06/InteligenciaArtificialNuriaOliver.pdf.

La inteligencia artificial es una herramienta que está permeando de forma constante nuestra vida, siendo cada vez una opción recurrente por su efectividad que sobrepasa -en algunos aspectos- la capacidad humana. Según Nuria (2020):

> Hoy podemos usar cantidades masivas de datos para entrenar algoritmos de Inteligencia Artificial, y hacer que decisiones que antes eran tomadas por humanos –con frecuencia expertos– recaigan sobre estos algoritmos. Pueden ser decisiones que afectan a una o muchas personas, y sobre cuestiones nada triviales, como la contratación laboral, la concesión de créditos y préstamos, sentencias judiciales, tratamientos y diagnósticos médicos o la compraventa de acciones en bolsa. (Nuria, 2020, p. 121)

Para concluir este capítulo, la forma en que entendemos las herramientas tecnológicas y el funcionamiento de las herramientas que utilizamos hoy en día, nos permite aproximarnos al contexto en donde nos desarrollamos como seres humanos, pues la Internet es el centro de interacción más importante en la actualidad, espacio en el cual ejercemos nuestros derechos de opinión, de información, de educación, entre otros; por lo tanto, el riesgo de que sean vulnerados crece de forma transversal al incremento de estas tecnologías, temas que se explicarán en los capítulos siguientes.

5. Marco Jurídico sobre la regulación de datos en Colombia

5.1.Habeas data (Ley 1581 de 2012)

El habeas data, del latín “Hábeas” (tráigase) y el del anglosajón “Data” (dato) puede definirse como un instituto jurídico que tiene como objetivo el acceso a la información, en virtud del derecho que tiene cualquier ciudadano a saber, actualizar, rectificar o eliminar datos personales recolectados y almacenados por terceros en bases de datos, sean de carácter financiero o no. (Pérez, 2017)

El ejercicio de este derecho implica velar porque la información personal otorgada a otros y recolectada en bases de datos o archivos sea recogida y tratada apropiadamente, bajo el

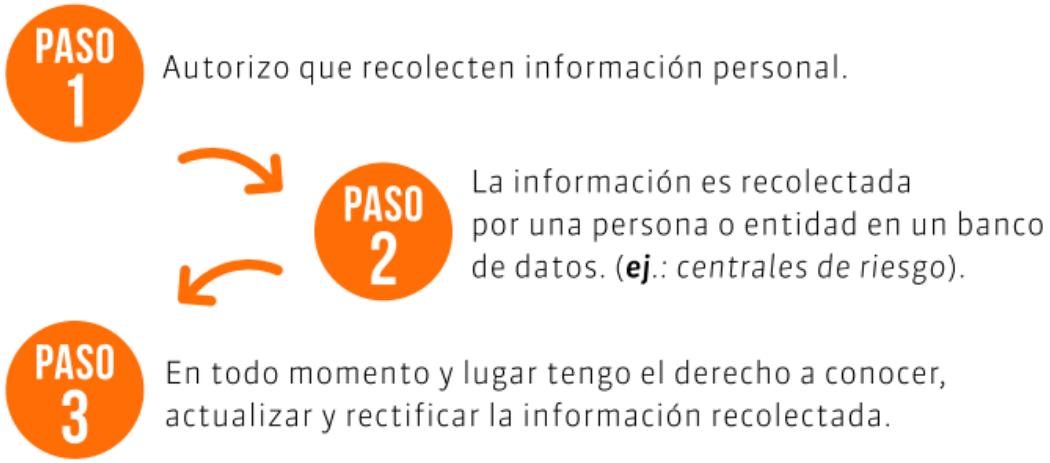
entendimiento de que el titular del derecho es el propietario de la información con todo lo que el derecho de dominio implica. El espacio de impacto del habeas data, incluye las plataformas digitales o redes sociales, tal cual como lo ha considerado la jurisprudencia de la Corte Constitucional, según la cual, los datos personales contienen las siguientes características:

> i) están referido a aspectos exclusivos y propios de una persona natural, ii) permitir identificar a la persona, en mayor o menor medida, gracias a la visión de conjunto que se logre con el mismo y con otros datos; iii) su propiedad reside exclusivamente en el titular del mismo, situación que no se altera por su obtención por parte de un tercero de manera lícita o ilícita, y iv) su tratamiento está sometido a reglas especiales (principios) en lo relativo a su captación, administración y divulgación. (Corte Constitucional, Sentencia C-748, 2011).

Siempre debe mediar la autorización expresa del titular para el tratamiento de datos personales, si se dan los presupuestos legales para ello, v. gr. Se trata información privada o semiprivada.

Figura 4.

Proceso de autorización de datos personales.



Nota: Proceso de autorización de datos personales según Cartilla expedida por la SIC. Adaptado de Superintendencia de Industria y Comercio (2020, pág. 4). https://www.sic.gov.co/sites/default/files/files/Nuestra_Entidad/Publicaciones/Aspectos_Derecho_de_Habeas_Data.pdf.

A su vez, cada que se entreguen este tipo de datos, se debe informar por la persona que los trate, el uso que se va a dar del mismo y que se solicite autorización expresa para el manejo de esta información circunscrito a unas finalidades. Hay algunos casos de naturaleza pública (Registro civil, información con fines históricos, estadísticos o científicos) en donde no se requiere la autorización expresa de su titular, de conformidad con el artículo 20 de la Ley 1581 de 2012 (Superintendencia de Industria y Comercio, 2010).

Como se evidencia, la protección de datos personales está asegurada según este derecho. Sin embargo, las líneas son difusas cuando son las mismas autoridades públicas las que hacen uso del mismo, pues puede generar consecuencias a futuro como indicios en investigaciones judiciales por comentarios en redes sociales; sobre este tema se abordará más adelante en el texto,

específicamente en el capítulo concerniente a la libertad de expresión. Ante ello, existen varias acciones judiciales como garantía de protección del derecho: i) el procedimiento sancionatorio administrativo ante la Superintendencia de Industria y Comercio, como Autoridad Nacional de Protección de Datos Personales; ii), la acción de tutela cuando se vulnere o amenace vulnerarse el habeas data y, iii) por medio de la acción de competencia desleal cuando el indebido tratamiento de datos personales constituya una violación de la ley que genere una ventaja significativa, en los términos del artículo 18 de la Ley 256 de 1996.

El desarrollo del habeas data se ha dado en su mayoría por la jurisprudencia de la Corte Constitucional, en la sentencia SU-139 del año 2021, se recogen varios de los conceptos que delimitan el habeas data, entendiéndolo con un derecho fundamental autónomo que busca proteger el dato personal, sus criterios de clasificación de datos corresponden a los siguientes:

- **Información pública o de dominio público:** información que puede ser obtenida sin reserva alguna, como documentos públicos, providencias judiciales, datos sobre el estado civil entre otros.
- **Información semiprivada:** referente a los datos que contengan información personal o impersonal, porque para obtener su acceso presentan algún tipo de limitación; por lo cuál solo puede ser obtenida y ofrecida por orden de autoridad administrativa en cumplimiento de sus funciones o en el marco de principios de administración de datos personales; por ejemplo, los datos referentes al comportamiento financiero de una persona.
- **Información privada:** Trata sobre la información personal -en un ámbito privado- y solo puede ser obtenida y ofrecida por orden de autoridad judicial en el cumplimiento de sus funciones, por ejemplo, los libros de comerciantes, documentos privados, e historias clínicas.

- **Información reservada:** la información reservada contiene información personal, lo conocido como "datos sensibles" relacionados con la ideología, inclinación sexual, hábitos de la persona. Ninguna autoridad judicial puede solicitarla en cumplimiento de sus funciones, pues afectan directamente la intimidad del titular, y su uso indebido puede generar discriminación. (T-020, 2014)

La Corte Constitucional ha recalcado que, en virtud del principio de libertad, el tratamiento de datos solo puede ejercerse con el consentimiento libre, previo y expreso del titular, a menos de que medie un mandato legal o judicial que revele el consentimiento; incluyendo el derecho del titular de disponer de la información y conocer su propia identidad informática, incluso en el ámbito de internet o redes sociales. (SU-139, 2021).

5.2.Ley 1341 de 2009

Esta ley define principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones –TIC–, y crea la Agencia Nacional de Espectro. Su objeto da un marco general para formular políticas públicas que rigen el sector de Tecnologías de la Información y las Comunicaciones, especialmente de la protección al usuario. Según su artículo 2° numeral 4, la protección de los derechos de los usuarios de las Tecnologías de la Información y de las Comunicaciones, como el cumplimiento de los deberes derivados del hábeas datas es una prioridad del Estado, por lo que los proveedores y/u operadores deberán prestar sus servicios a precios de mercado y utilidad razonable, brindando información clara, transparente y necesaria, y el principio de neutralidad tecnológica. (Art 2, numerales 4° y 6°)

5.3.Ley estatutaria de 1581 de 2012

En concordancia con este principio, la Ley Estatutaria 1581 de 2012 "Por la cual se dictan disposiciones generales para la protección de datos personales" tiene como objeto desarrollar el

derecho de habeas data, teniendo como ámbito de aplicación los datos personales tratados en cualquier base de datos o ficheros, que se hagan susceptibles de tratamiento por entidades de naturaleza pública o privada (Art 2), siguiendo el principio de "Acceso y circulación restringida".

> **Principio de acceso y circulación restringida:** El Tratamiento se sujeta a los límites que se derivan de la naturaleza de los datos personales, de las disposiciones de la presente ley y la Constitución. En este sentido, el Tratamiento sólo podrá hacerse por personas autorizadas por el Titular y/o por las personas previstas en la presente ley.
>
> Los datos personales, salvo la información pública, no podrán estar disponibles en Internet u otros medios de divulgación o comunicación masiva, salvo que el acceso sea técnicamente controlable para brindar un conocimiento restringido sólo a los Titulares o terceros autorizados conforme a la presente ley. (Ley 1581, 2012. Art 4° numeral f)

Según el MinTIC, esta ley reconoce y protege el derecho que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos que sean susceptibles de tratamiento por entidades de naturaleza pública o privada. Los datos personales conforman la información necesaria para que una persona pueda interactuar con otros o con una o más empresas y/o entidades, para que sea plenamente individualizada del resto de la sociedad, haciendo posible la "generación de flujos de información que contribuyen con el crecimiento económico y el mejoramiento de bienes y servicios", por ejemplo, en la compra de bienes en internet. (MinTIC, 2022)

5.4.Ley 1712 de 2014

Siguiendo con los principios de transparencia, en el marco de la misma se creó la ley 1712 de 2014: "*Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la*

Información Pública Nacional y se dictan otras disposiciones". La máxima publicidad es predicable de todas las instituciones públicas, en principio, derivándose de la misma deberes como los de transparencia, facilitación, buena fe, no discriminación, celeridad, gratuidad, eficacia y calidad de la información (Art 3). En virtud del derecho fundamental al acceso a la información, toda persona puede conocer sobre la existencia y acceder a la información pública en posesión o bajo control de los sujetos obligados, solo puede ser restringido de forma **excepcional,** generando también la obligación de divulgar proactivamente la información pública y responder de buena fe (Art 4°). Su excepción solamente se da en los casos de información clasificada y reservada, como la que puede causar daño a los intereses públicos. En todo caso, el solicitante de información puede interponer, de forma inmediata ante la entidad una queja o reclamo; en caso de que el mismo sea infructífero puede procederse por medio del recurso de reposición o los que procedan legalmente, cuando se dan respuestas sin sustento sobre la negativa, el mismo debe interponerse por escrito y si se niega, se puede acudir al Tribunal Administrativo con jurisdicción en el lugar donde se encuentren los documentos (Art 27°).

5.4.1. Transparencia de Instituciones públicas: caso Comisión de la verdad (en liquidación).

Durante la práctica en Dejusticia, la Comisión de la verdad solicitó a la línea de Tecnología, Transparencia y Derechos Humanos, orientación sobre el modo de difusión de la información recolectada en el marco de sus funciones como Comisión de la Verdad, cuya creación se dio en el marco del Acuerdo Final para la Terminación del Conflicto y la Construcción de una Paz Estable y Duradera: este acuerdo fue suscrito entre el Gobierno de Colombia y las Fuerzas Armadas Revolucionarias de Colombia – FARC-EP (Acto legislativo 01, 2017). El mismo estuvo en funcionamiento con el objeto de esclarecer los patrones y causas explicativas del conflicto armado interno, que satisfaga el derecho de las víctimas y de la sociedad a la verdad, el reconocimiento de

lo sucedido y la convivencia para la construcción de paz (Comisión de la verdad, 2022). Su carácter era temporal (3 años). Sus hallazgos sobre el conflicto contienen información sensible de las víctimas, por lo que fue necesario buscar y aplicar métodos de anonimización para mantener la información reservada. Este trabajo fue hecho por Juan Carlos Upegui y Daniel Ospina y mi participación consistió en supervisar y verificar que en efecto se haya construido el archivo final respetando el test de daño y la construcción sugerida por Dejusticia. Las reuniones de socialización del informe final se dieron en el mes de marzo y abril del año que avanza, en las cuales se analizó el objetivo planteado. El índice es accesible a la población colombiana, que se encontrará disponible en el siguiente link: https://archivo.comisiondelaverdad.co/. La Comisión de la Verdad presentó su informe final en mayo de 2023, entregando el reporte completo al Archivo General de la Nación[9].

La distinción de cada una de las leyes de protección de datos no trae consigo la definición explicita del espacio global y controvertido de internet, a pesar de que es mencionado, sobre el mismo no se profundiza de una manera que deje entender la regulación y recolección de datos en la red. Existe un marco de regulación especifico en los temas que se van a tratar durante el texto (libertad de expresión, brecha digital, inteligencia y protección de datos de los usuarios en internet).

6. Libertad de expresión, desinformación y discursos de odio.

[9] La socialización del índice se dejará en los anexos correspondientes, el mismo se socializó en reuniones de carácter interno promovidas por la Comisión de la Verdad (en liquidación) en las cuales se participó como representante de la línea de tecnología y derechos humanos.

Para empezar, partimos de la idea de las plataformas digitales (específicamente redes sociales) para el ejercicio de múltiples derechos, siendo uno de los más relevantes, el derecho a la libertad de expresión, consagrado en el artículo 20 de la Constitución Política de Colombia.

> *ARTICULO 20.* Se garantiza a toda persona la libertad de expresar y difundir su pensamiento y opiniones, la de informar y recibir información veraz e imparcial, y la de fundar medios masivos de comunicación. Estos son libres y tienen responsabilidad social. Se garantiza el derecho a la rectificación en condiciones de equidad. No habrá censura. (Const., 1991. Art 20)

6.1.Libertad de expresión, libertad de opinión e información.

Naciones Unidas ha analizado de forma extensa el tema de la libertad de expresión, especialmente en los informes dados por el Reportero Especial en la promoción y protección del derecho a la libertad de ***opinión*** y ***expresión***. Según Frank La Rue (2011) el derecho protegido por el artículo 19 de la Declaración Universal de los Derechos Humanos, correspondiente a la libertad de expresión:

> "Todo individuo tiene derecho a la libertad de opinión y de expresión; este derecho incluye el de no ser molestado a causa de sus opiniones, el de investigar y recibir informaciones y opiniones, y el de difundirlas, sin limitación de fronteras, por cualquier medio de expresión". (ONU, 1948)

En concordancia con esta definición, la Corte Constitucional ha reiterado la característica polifacética de este derecho, incluyendo la libertad de expresar ideas y opiniones (libertad de opinión), como la libertad de difundir y recibir información, la libertad de prensa, la rectificación en condiciones de equidad y la prohibición de censura. De acuerdo a lo considerado en la sentencia T-063A (2017):

> En el marco de la jurisprudencia constitucional colombiana, la Corte Constitucional ha sostenido que la garantía a la libertad de expresión comprende dos aspectos distintos, a saber: ***la libertad de información,*** orientada a proteger la libre búsqueda, transmisión y recepción de información cierta e imparcial sobre todo tipo de opiniones, incluyendo hechos e ideas. El segundo aspecto, es aquel que hace referencia a ***la libertad de opinión***, entendido como libertad de expresión en sentido estricto, el cual implica básicamente la posibilidad de poder difundir o divulgar, a través de cualquier medio de comunicación, las propias ideas, opiniones y pensamientos. (Corte Constitucional, T-063A; 2017)

En redes sociales, se remarca más aún la dimensión individual de este derecho, que abarca tanto el hecho de expresarse sin interferencias arbitrarias, como el derecho a utilizar cualquier medio apropiado para difundir su pensamiento. (Corte Constitucional, T-203; 2022)

En caso de llegar a limitar la libertad de expresión, se debe hacer siguiendo un test tripartito:

- Legalidad: asesoramiento de legalidad, en donde el intermediario debería analizar si la interferencia con las ideas expresadas puede regularse por medio de leyes existentes.
- Necesidad: analiza si el discurso utilizado es el instrumento menos intrusivo para lograr este medio.
- Proporcionalidad: no se puede incidir de manera excesiva en el ejercicio de este derecho fundamental. **(U.N, GAOR; sesión 102, 2011)**

Por otro lado, la Corte Constitucional también afirma que en caso de que se pretenda cuestionar o restringir la libertad de expresión, debe seguirse el principio de supremacía de la libertad de expresión (prima facie), la presunción legal sobre la inconstitucionalidad de las

limitaciones sujetas a un control estricto de proporcionalidad, sin llegar nunca a recaer en la censura previa (la cual es una presunción de pleno derecho). (Corte Constitucional, T-203; 2022)

Los actores internacionales han exhortado a la revisión de políticas de moderación de contenidos, en la jurisprudencia de la CIDH., Específicamente la relatoría elaborada por Edison Lanza[10] se aclara de forma precisa que la protección del derecho de la libertad de expresión va incluso hasta los discursos con expresiones chocantes, que generan controversia, o discursos incluso equivocados, pues si bien generan una responsabilidad ulterior, deben ser protegidas en el marco de una sociedad democrática, abierta, plural y tolerante. En opinión de Lanza (2016) solo es proceden recurrir a medidas como bloqueo de cuentas o eliminación:

> (…) cuando se está frente a contenidos abiertamente ilícitos o a discursos no resguardados por el derecho a la libertad de expresión (como la propaganda de guerra y la apología del odio que constituya incitación a la violencia, la incitación directa y pública al genocidio, y la pornografía infantil). (p. 34)

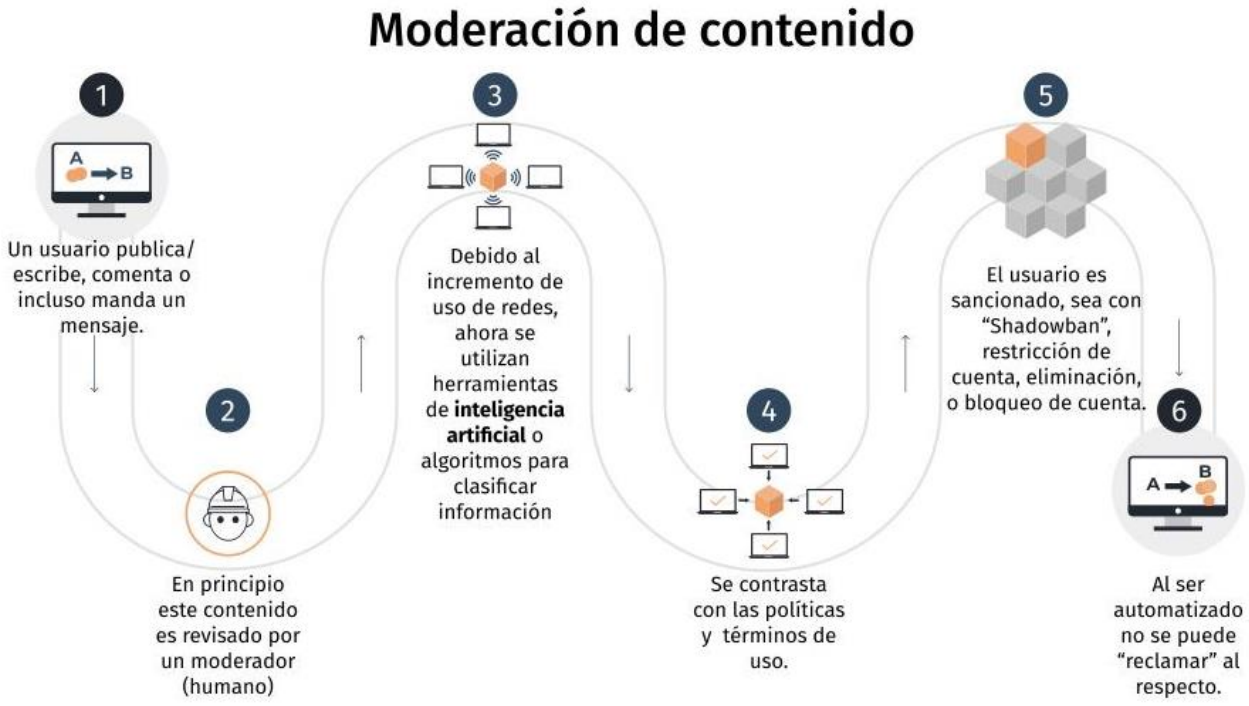
6.2.Moderación de contenido

La implosión de usuarios en las plataformas de redes sociales equivale a que las políticas de regulación aumenten, dado que en su mayoría las compañías no regulan este contenido directamente, pues hay terceros que trabajan como contratistas de la institución para filtrar los contenidos.

Figura 5.

Moderación de contenido en redes sociales.

[10] Ex relator Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos.



Nota: Adaptado de "Moderación privada de contenidos en Internet y su impacto en el periodismo" (Pérez & Martínez, 2022). Elaboración propia.

El uso de algoritmos en tecnología cobra un papel importante en las redes sociales, pues su uso varía desde la selección de información relevante para usuarios, hasta identificación de "contenido inapropiado", según Dias Oliva (2020):

> Los algoritmos analizan datos recolectados de un usuario a otro, recomendando contenidos similares que estén dentro del rango de sus gustos; estas tecnologías trabajan de forma automática sin intervención humana (…) Considerando su facilidad de construcción a escala, los algoritmos están siendo utilizados para la eliminación de contenido, donde Facebook o Youtube implementan algoritmos para la eliminación de contenido protegido por copyright, propaganda terrorista, imágenes NSFW. (p. 3)

Los análisis a estándares de uso de redes sociales como Facebook o Twitter cada día son cuestionados, pues pasaron de una obligación de control a una eliminación sistemática por análisis que ni siquiera es hecho por humanos, que no muestra tampoco un régimen concreto de transparencia e incumplen los estándares mínimos del debido proceso, como son la notificación oportuna a los usuarios sobre la violación de estándares comunitarios y la oportunidad que se dé de apelar a esta medida (CIDH, 2017)

6.3.Limitación a libertad de información / elección

Otro aspecto a resaltar sobre los términos de uso y la utilización de algoritmos es la limitación -no solo de la libertad de expresión- sino de elección. La jerarquización y procesamiento de contenido hacen que estos espacios funcionen de forma más limitada, que puede llegar a tener un impacto en la formación y deliberación democrática, pero ¿*por qué*?

El personalizar contenido hace que limitemos nuestra opinión a sólo nuestros intereses; por lo tanto, la presentación de ideas contrarias a las que estamos habituados, crea -inevitablemente- una reacción de intolerancia. Retomando a Cobo (2023), para que exista una democracia deben confrontarse ideas diferentes, sin que necesariamente se cancelen la una a la otra.

Uno de los ejemplos más preocupantes sobre la limitación de la libertad de elección -democracia- se dio en las elecciones estadounidenses del 2016 (Donald Trump vs Hillary Clinton), cuando la empresa Cambridge Analytica dirigió un experimento de recolección de datos, donde se analizaba la cantidad de votantes “indecisos” y se influía en sus decisiones para que votaran por cierto partido político, siguiendo la lógica de la personalidad de cada votante. Lo anterior, acorde a los datos extraídos de sus redes sociales -desde publicaciones, hasta conversaciones privadas-, combinando la información a su alcance, la psicología conductual y la hipersegmentación que se

llevaba a cabo en el proceso. Con estas tácticas se pudo llegar a personas concretas mediante contenido (publicidad) altamente personalizada. Estos *ads*[11] contenían vídeos, imágenes, recomendaciones de grupos sociales. Difiere del concepto originario de libertad de información o acceso a la misma, pues específicamente estaban intencionados a la influencia para un interés privado (elección de un candidato presidencial)[12]. (Amer, & Noujaim, 2019)

Esto se dio gracias al principio de funcionamiento de redes sociales, en donde se toma el tiempo de atención del usuario, en donde su participación e involucramiento directo se verán incrementados si se encuentran contenidos con los cuales se identifique, guiándose por la oferta de contenidos que a su vez consumen sus amigos y referentes cercanos.

Según PNUD[13] (2021):

> En este escenario, el modelo de negocios basado en la acumulación de datos genera fragmentación, y los algoritmos y la inteligencia artificial son guiados por valores más relacionados a uniformidad y semejanza que a valores de pluralismo y diversidad (…) Esta contradicción está directamente relacionada con el objetivo de mantener el usuario más tiempo en la plataforma. Así, la fragmentación y segmentación son fenómenos que se refuerzan en espiral, y refuerzan lo que estudiosos denominan como filtros burbuja y cámaras de eco. (p. 22)

[11] Término utilizado para referirse a anuncios en redes sociales, proviene de la palabra *"advertising*" que significa publicidad.

[12] Este caso se hizo de conocimiento público gracias al documental de Netflix llamado "The Great Hack", centrado en David Caroll y Brittany Kaiser, que participaron en el proyecto conocido como Cambridge Analytica, encargados de analizar macro-datos para estrategias de venta masiva a usuarios y campañas políticas como el Brexit en Reino Unido y las elecciones presidenciales de Estados Unidos en 2016.

[13] Programa de Naciones Unidas para el desarrollo en Uruguay.

Como se evidencia, contraría la base esencial de un régimen democrático, como lo resaltó la CIDH (2007), en el marco de una campaña electoral debe primar siempre la libertad de pensamiento y de expresión en sus dos dimensiones, debido a que es una herramienta especial para la formación pública de electores, como la responsabilidad de los candidatos políticos de respetar opiniones contrarias y generar una contienda transparente. (CIDH, 2007)

6.4.Intervención gubernamental

Otro actor por el cual la relatoría de la CIDH muestra gran preocupación es el Estado. En varias ocasiones las empresas de redes sociales como META o Twitter se ven obligadas a adaptar las políticas de moderación de contenido según los intereses de un gobierno específico; las cuáles censuran contenido "inapropiado" cuando se habla en contra de determinado gobierno, o la creación de filtros que permitan dar de baja contenidos relacionados con situaciones sociales (ONU, 2020). Asimismo, hay un cerco en el tipo de acceso a la información establecida, pues el porcentaje de países investigados contra la vulneración sistemática de este derecho, se dieron principalmente en este contexto; tomando como ejemplo más representativo, el caso Myanmar[14].

Según la relatoría especial de David Kaye, las preocupaciones principales sobre cómo se regula el contenido y la intervención de dichas empresas intermedias debe seguir un orden estricto, en donde se manifieste la ilegalidad total de representaciones de abuso sexual infantil, amenazas directas de muerte (creíbles), e incitación a la violencia directa.

[14] El caso Myanmar aborda el genocidio de la comunidad Rohinyá en el país, Facebook era la única plataforma a la cuál accedían en el país para informarse o expresar opiniones, sin embargo, el Gobierno Birmano -por medio de cuentas falsas- difundió el discurso de odio contra la comunidad, generando así que se desataran crímenes de lesa humanidad, por los cuales el Estado de Myanmar fue acusado. (ONU, 2020)

Los Estados deben evitar la persecución y la censura para regular este tipo de plataformas, Colombia, se ha tratado el tema de políticas de uso y libertad de expresión en la jurisprudencia dada por la Corte Constitucional, con criterios de unificación respecto a lo que puede significar la injuria y calumnia, con respecto a la moderación de contenido, cada plataforma está comprometida -prima facie- a respetar las leyes locales, sin embargo esto puede resultar difícil de hacer si no hay una legislación definida sobre conceptos referentes a extremos, pues varios reportes hechos por las empresas de tecnología muestran la presión que los Gobiernos locales ponen en estas plataformas para eliminar contenido, suspender cuentas o compartir información confidencial (UN, AHRC 38/35; 2018)

6.5.Transparencia en las redes sociales

La solución al problema de acceso a la información y moderación de contenidos, analizada desde la línea de tecnología, transparencia y derechos humanos; es precisamente a la Transparencia. El trabajo continuo de las instituciones por proveer datos reales al público sobre el consumo de información y utilización de datos es vital para garantizar el uso adecuado de las redes sociales, a pesar de los intentos de las mismas plataformas por explicar sus condiciones de uso (artículos y blogs) las mismas aún necesitan un cuerpo de *soft law*, es decir, una guía de buenas prácticas, para que así puedan tener un marco mínimo de obligaciones para brindar información a la ciudadanía.

A su vez, se debe implementar conceptos conocidos como "debida diligencia"[15], implementando criterios utilizados en la investigación desde derechos humanos. Para ello, las compañías deben desarrollar criterios y procesos que puedan ser curados por los mismos usuarios, y contener asesoramiento de Organizaciones Multilaterales que provean una visión más amplia al respecto, evaluando el impacto real de dichas políticas en la sociedad civil. La prioridad siempre será analizar de forma concienzuda, respetando el contexto social de cada país en particular. Es necesario regular también la explicación por eliminación de contenidos, suspensión de cuentas y limitación de uso en redes sociales; pues este escenario puede llegar a convertirse en un panorama totalitario, en donde cabe la pregunta de la necesidad de un cierto tipo de figura judicial que pueda dirimir este tipo de conflictos, toda vez que hay un desequilibrio evidente entre la parte indefensa que es el usuario, frente a plataformas como Meta o Twitter. (UN, AHRC 38/35; 2018)

6.6.Transparencia en la legislación colombiana

La ley 1712 de 2014 creó la "Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional", en concordancia a las sugerencias a políticas públicas hechas por organismos multilaterales, entre los cuáles se establecen los principios base de transparencia, buena fe, facilitación, no discriminación, gratuidad, celeridad, eficacia, calidad de información, divulgación proactiva de la información, y responsabilidad en el uso de la información. En cuanto a la definición del principio de transparencia, la ley consagró lo siguiente:

[15] Según Amaya y Zuluaga (2022): El significado del término hace referencia a la actuación de acuerdo con un cierto estándar de cuidado. Este cierto estándar de cuidado ya aparece recogido en otras esferas del derecho, pero en relación con las empresas y los derechos humanos son los Principios Rectores de Naciones Unidas quienes introducen este concepto, a pesar de que no proporcionan una definición.

> **Principio de transparencia:** Principio conforme al cual toda la información en poder de los sujetos obligados definidos en esta **ley se presume pública**, en consecuencia, de lo cual dichos sujetos están en el **deber de proporcionar y facilitar el acceso a la misma en los términos más amplios posibles** y a través de los medios y procedimientos que al efecto establezca la ley, excluyendo solo aquello que esté sujeto a las excepciones constitucionales y legales y bajo el cumplimiento de los requisitos establecidos en esta ley. (Ley 1712, 2014. Art 3)[16]

En concordancia a ello, también consagra en el parágrafo subsiguiente el Principio de facilitación: "En virtud de este principio los sujetos obligados deberán ***facilitar el ejercicio del derecho de acceso a la información pública***, excluyendo exigencias o requisitos que puedan obstruirlo o impedirlo" (Ley 1712, 2014. Art 3)[17].

Por otro lado, la información difundida debe ser oportuna, objetiva, veraz, completa, reutilizable, procesable, y estar disponible en los formatos accesibles, culminando con la responsabilidad estatal de divulgar de forma proactiva esta información, siendo accesible por todo el público, sin necesidad de derechos de petición como intermediario. Esta ley aborda el carácter obligatorio de las instituciones públicas a difundir información transparente y de confianza, exceptuando información que esté clasificada, que pueda llegar a causar daño a personas naturales o jurídicas o por daño a los intereses públicos.

[16] Subrayas fuera del texto original.

[17] Subrayas fuera del texto original.

Sin embargo, según investigaciones hechas por Dejusticia (Newman et al, 2020) (Newman & Angel, 2020), se evidencia que el cumplimiento de parámetros de transparencia (que se deberían aplicar en redes sociales y a organismos multilaterales) son incumplidos de forma sistemática por el Estado Colombiano. En tal sentido, la organización y clasificación de información debe seguir instrucciones en particular que correspondan a la garantía de derechos humanos. No obstante, las políticas para acceso de información incluso de instituciones como Universidades Públicas o Fiscalía[18], son limitadas y puestas en cuestionamiento por autoridades, evidencia que se dio en el marco de la práctica al enviar derechos de petición a las dos Instituciones, solicitando datos como ganancias percibidas por los funcionarios o funcionamiento interno de la institución; peticiones que fueron cuestionadas y denegadas por las dos Instituciones, creando así obstáculos en la comunicación y proliferación de una mayor transparencia en los datos.

7. Vigilancia estatal

Se ha mencionado a un rango extenso sobre el papel de las Empresas de Tecnología en la forma como percibimos el contenido que consumimos y cómo interactuamos con el mismo. Sin embargo, un papel importante -y crucial dentro del análisis hecho desde Dejusticia- concierne al Estado, específicamente se abordarán los mecanismos de vigilancia estatal ejercidos por Inteligencia y diferentes corporaciones que tienen control de datos; que pueden significar

[18] Este análisis fue hecho durante el seminario acotado del texto "La Fiscalía General de la Nación y la investigación de la corrupción: obstáculos y buenas prácticas"; promovido dentro de la línea de Tecnología, Transparencia y DDHH, en conjunto con la línea de Sistema Judicial de Dejusticia y la Institución Transparencia por Colombia. El texto se encuentra en fase de edición, se puede consultar una vez esté publicado en la página oficial de Dejusticia.

consecuencias graves en la afectación de derechos humanos como la privacidad, ya que el manejo de tecnologías de vigilancia estatal ubicuas vulneran sus datos personales, contraseñas, ubicación geográfica y mensajes personales.

7.1.Derecho a la privacidad

El derecho a la intimidad es un derecho humano fundamental, reconocido en numerosos instrumentos internacionales de derechos humanos, esencial por su conexidad con ottos derechos como la dignidad humana, libertad de expresión, información y asociación. La Constitución Política de 1991, en su artículo 15, consagra el derecho a la "intimidad" de la siguiente forma:

> Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas.
>
> En la **recolección, tratamiento y circulación de datos se respetarán la libertad** y demás garantías consagradas en la Constitución. La correspondencia y demás formas de comunicación privada son inviolables. Sólo pueden ser interceptadas o registradas **mediante orden judicial**[19], en los casos y con las formalidades que establezca la ley. (CP, 1991. Art 15)

La observancia del derecho a la intimidad permite que se cuente con una esfera o espacio de vida privada, sin ser susceptible de interferencia arbitraria de las demás personas, y el mismo

[19] Subrayas resaltadas fuera del texto original.

solo puede ser objeto de limitaciones si se tiene un verdadero interés general que responda a los presupuestos establecido por la Constitución y la ley (Corte Constitucional, C-640; 2010)

Precisamente esta amplia definición de regulación en carácter de privacidad, crea una extralimitación de funciones por parte de las autoridades públicas, pues al no existir una regulación limitada, se considera a criterio de dichas autoridades el contenido que ellos quieran clasificar, regular, censurar, etc. (Camacho et al, 2023) A pesar de que exista el mandato expreso de mediación de orden judicial, las mismas varían acorde a las circunstancias, incluso deben seguir la observancia de varios principios:

1. *Principio de finalidad:* solo se debe someter la recopilación y divulgación de datos si existe un fin constitucionalmente legítimo.
2. *Principio de necesidad:* la información personal divulgada debe ser estrictamente la que guarda relación con la finalidad pretendida.
3. *Principio de veracidad:* exige que los datos personales que se puedan divulgar correspondan a situaciones reales.
4. *Principio de integridad:* según la cual la información que sea objeto de divulgación debe suministrarse de manera completa, impidiendo que se registre y divulgue datos parciales incompletos o fraccionados. (Corte Constitucional, C-640; 2010)

El concepto de intimidad viene asociado al de soberanía sobre un territorio cerrado, asociándose a las estructuras democráticas y liberales, lo privado es un ámbito restringido. A pesar de que en la posmodernidad se extrapolen las definiciones de lo que es “privado” o lo que no, el deber del Estado (en principio) es de respetarlo y garantizarlo en todas sus esferas. Al respecto

aparece el concepto de “expectativa razonable de intimidad” la cual refiere a una zona de protección garantizada en el que el individuo puede actuar basado en la confianza legítima de que no habrá injerencias del estado o de terceros. Según la Corte Constitucional (2022):

> El derecho a la intimidad evolucionó desde su dimensión más individual a la que correspondían fundamentalmente obligaciones negativas de los particulares y del Estado hacia una concepción amplia, social o relacional. A esta no solo se le adscriben deberes de abstención sino obligaciones positivas del Estado. Finalmente, queda muy claro que este derecho se proyecta tanto en los lugares públicos como en los privados porque en todos estos existe una expectativa razonable y diferenciada de intimidad. Como se indicará en la siguiente sección, la jurisprudencia constitucional sobre el derecho a la intimidad ha seguido esta misma evolución del derecho comparado e internacional de los derechos humanos. (Corte Constitucional, T-280, 2022)

A pesar de la referencia de la norma en protección de espacios públicos o privados, se tiene en cuenta que la internet es un espacio también de interacción, el cual crea una extensión a su protección en la expectativa razonable de privacidad. Sobre el particular, la sentencia C-1147 de 2001, manifestó que aun cuando en Internet se represente un espacio virtual, los derechos de las personas no son “virtuales” o abstractos, se trata de garantías expresas por cuyo goce efectivo en el ciberespacio es objeto de protección constitucional. (Corte Constitucional, C-1147, 2001)

7.2.Vigilancia Estatal: Inteligencia y Contra Inteligencia

Ya se había mencionado anteriormente de la capacidad de las empresas de GAFAM de tomar la geo-localización de sus usuarios y ejercer un seguimiento, incluso cuando no estamos conectados a una red de WiFi o datos móviles. La recolección de los datos que normalmente

forman parte de nuestra vida cotidiana se conoce como "*excedente conductual"*[20], algo que no solamente utilizan las empresas de tecnología, sino el Estado.

Muchas veces existe una alianza entre las mismas, según lo recalca el relator especial (2019):

> Los gobiernos y el sector privado colaboran estrechamente en el mercado de los instrumentos para la vigilancia digital. Los gobiernos tienen necesidades que sus propios departamentos y agencias no pueden satisfacer. Las empresas privadas tienen los incentivos, la experiencia y los recursos necesarios para satisfacerlas. Se reúnen en ferias comerciales de ámbito mundial y regional diseñadas, como los servicios de citas, para que puedan juntarse. A partir de ahí, determinan si pueden formar una pareja. Se desconoce si las empresas llevan a cabo algún tipo de diligencia debida para evaluar la trayectoria de los compradores en materia de derechos humanos. (U.N, A/HRC/41/35; 2019)

Desde antaño se han llevado a cabo operaciones de inteligencia, espionaje e interceptación por parte del Estado hacia individuos o a otros Estados, normalmente estas prácticas forman parte de una "zona gris" en donde todo parece estar permitido. Con la creciente ola de tecnología y la hiperconectividad a la cual estamos sometidos diariamente, la vigilancia Estatal que se ejercía de forma antigua mediante objetos específicos, hoy en día, se convirtió en una herramienta que -a

[20] Según Zuboff (2020), los datos se analizan a partir del comportamiento de los usuarios, por lo tanto, su excedente conductual corresponde a los patrones de comportamiento que permiten una predicción sobre los gustos de la persona, estos datos son precisamente los de nuestra convivencia "con el mundo real", nuestras conversaciones con amigos, familiares, la ropa que usamos, la ubicación de los muebles, entre otros.

prevención- puede causar repercusiones no solo en la privacidad, sino incluso en el debido proceso y presunción de inocencia.

Según reporte elaborado por la ONU (2019):

> La vigilancia de personas concretas —a menudo periodistas, activistas, personalidades de la oposición, críticos y otras personas que ejercían su derecho a la libertad de expresión— ha conducido en ocasiones a la detención arbitraria, a veces a la tortura y tal vez a ejecuciones extrajudiciales. Esas actividades de vigilancia han prosperado en medio de la debilidad de los controles sobre la transferencia de tecnología a gobiernos con políticas de represión conocidas. Ese mercado está envuelto en un velo de secretismo. (U.N, A/HRC/41/35; 2019)

A pesar de lo abordado con respecto a la transparencia de Instituciones Públicas, este régimen no es aplicable tratándose de instituciones de inteligencia y contrainteligencia (Fuerzas Militares, Policía Nacional, Unidad de información y análisis financiero), pues las mismas poseen su propia regulación, la cual deja la pregunta sobre su ambigüedad manifiesta.

En el caso Colombiano, hasta el año 2013 se regularon las actividades de inteligencia por medio de la ley 1621 de 2013, que consagra lo siguiente en su artículo 2:

> La función de inteligencia y contrainteligencia es aquella que desarrollan los organismos especializados del Estado del orden nacional, utilizando medios humanos o técnicos para la **recolección, procesamiento, análisis y difusión de información, con el objetivo de proteger los derechos humanos**[21], prevenir y combatir amenazas internas o externas

[21] Subrayas fuera del texto original.

> contra la vigencia del régimen democrático, el régimen constitucional y legal, la seguridad y la defensa nacional, y cumplir los demás fines enunciados en esta ley. (Ley 1621, 2013. Art 2)

La función que cumplen es de carácter fundamental, pero los límites de investigación llevados a cabo por dichas Instituciones pueden extrapolar el objetivo principal de proteger derechos humanos, y llegar, en determinado caso, a vulnerarlos. Este análisis parte de la investigación realizada por Lucía Camacho, Daniel Ospina-Celis, y Juan Carlos Upegui (2023) en Dejusticia, a partir del caso denominado por la revista *Semana* como "carpetas secretas" (Semana, 2020) en el cual las instituciones de Inteligencia y Contra-inteligencia habían creado perfiles de varios periodistas, clasificándolos según sus publicaciones en redes sociales, sus contactos más cercanos y su actividad en plataformas como Facebook. La justificación para tal proceder se basó en que eran datos de acceso público, buscado por fuentes abiertas. Entonces si se trataba de fuentes abiertas, ¿cómo nuestras publicaciones pueden ser flancos para apuntalar investigaciones militares posteriormente? (Camacho et al, 2023)

El diseño institucional sobre recolección y tratamiento de datos puede ser tan diverso como complejo, pues la Ley específica los límites de la Constitución y la ley (Art 5). Empero, la reserva sobre su contenido impide que se pueda hacer una observancia efectiva del cumplimiento de observancia de la norma. En casos como el ejercicio de esta actividad en la recolección y tratamiento de información en línea o redes sociales, se parte del principio de que esta actividad no es consentida por el titular de los datos, y según entrevistas a los mismos integrantes de dichas instituciones, el ejercicio de estas actividades "trasciende a los intereses y actores en materia de

protección de la seguridad y defensa nacional" (Camacho et al, 2023. Pág. 22) Traduciéndose en el uso para investigación criminal o *ciberpatrullaje*[22].

La mayoría del perfilamiento realizado se dio con la intención de perfilar posturas políticas, que se comparten de forma pública ejerciendo el derecho de libertad de expresión, en estos casos su expectativa no es la de ser un objeto de monitoreo y perfilamiento por parte del Estado. Según la Corte Suprema de Justicia, independientemente que la información contenida en trinos pueda ser consultados abiertamente por el público, las entidades gubernamentales o empresas especializadas en la recolección de datos, no están facultadas para hacer uso de la misma como si se tratase de datos de naturaleza pública y con fundamento en ello elaborar listados de "influenciadores" según su ideología política, plasmada en su interacción en Twitter. (Corte Suprema de Justicia, STP9319, 2020)

Siguiendo con el tenor de las investigaciones dadas por Inteligencia Estatal, afirman de forma explícita no distinguir entre el entorno *físico* y el entorno *digital*, cuando se trata de recoger información con fines de inteligencia, la búsqueda de información se realiza con regularidad, en búsqueda de "fenómenos u amenazas que puedan atentar con valores constitucionales, legales, democráticos o de defensa nacional) (Chamacho, et al. 2023. Pág. 25).

7.3. Ciberpatrullaje

Según la resolución 5839 de 2015, el ciberpatrullaje corresponde a:

[22] Según Fundación Karisma (2023): el ciberpatrullaje consiste, normativamente, en una revisión de internet por parte del CAI virtual para identificar posibles delitos informáticos, ya que son estos últimos los que ponen en riesgo la ciberseguridad ciudadana.

> Un conjunto de actividades dirigidas a identificar amenazas e incidentes de ciberseguridad, así como a detectar la vulneración de la disponibilidad, integridad y confidencialidad de la información que circula en internet. (Resolución 5839, 2015)

Las actividades de ciberpatrullaje comprenden la consulta, observación y recolección de información en línea sobre datos y contenidos abiertos y públicos en internet y en redes sociales, contando el número de publicaciones, interacciones y visualizaciones (FLIP, 2021). La ley 1621 de 2013, en su artículo 17 consagra la actividad de "monitoreo del espectro electromagnético e interceptaciones de comunicaciones privadas".

> Las actividades de inteligencia y contrainteligencia comprenden actividades de monitoreo del espectro electromagnético debidamente incorporadas dentro de órdenes de operaciones o misiones de trabajo. La información recolectada en el marco del **monitoreo del espectro electromagnético** en ejercicio de las actividades de inteligencia y contrainteligencia, que no sirva para el cumplimiento de los fines establecidos en la presente Ley, deberá ser destruida y no podrá ser almacenada en las bases de datos de inteligencia y contrainteligencia. El monitoreo no constituye interceptación de comunicaciones.
>
> La interceptación de conversaciones privadas telefónicas móviles o fijas, así como de las comunicaciones privadas de datos, deberán someterse a los requisitos establecidos en el artículo 15 de la Constitución y el Código de Procedimiento Penal y sólo podrán llevarse a cabo en el marco de procedimientos judiciales. (Ley 1621, 2013. Art 17)

El no tener una limitación específica sobre el espectro electromagnético hace que la distinción hacia lo que acceden o usan -sin autorización- sea bastante amplio. Según Botero (2020) el limitar su definición haría que fuese parte de -al menos- un control judicial, pues este monitoreo incluye el de inteligencia en las redes sociales. En este caso no sólo se trata de recopilación de

datos, sino *de investigación criminal,* que está enfocada en recabar elementos probatorios que puedan ser valorados en juicio, para determinar -eventualmente- la responsabilidad penal de una persona, la misma está limitada por el marco del debido proceso, pues no pueden ser incorporadas en juicio si no se siguen estas reglas. (Corte Constitucional C-913, 2010)

La utilización del ciberpatrullaje tomó fuerza con la pandemia de la covid-19, pues la policía hacia una pesquisa exhaustiva de noticias falsas acerca del COVID-19. Empero, dicha práctica trascendió incluso hasta el Paro Nacional del año 2021, en donde la policía ejercía monitoreo sobre diferentes perfiles de información, activando más de 21.000 horas de vigilancia digital continua (Mindefensa, 2021). Además, esta actividad difirió de su intención inicial, la cual es rastrear "ciberdelitos". La consideración uniforme del espacio físico como el virtual crea potenciales consecuencias e impactos en la protección de nuestra privacidad, y también por la cantidad importante de información que se puede procesar en este espacio. Según la Fundación Karsima (2023):

> Pretender que el ciberpatrullaje es el mismo patrullaje, pero en espacios virtuales, es erróneo debido a la capacidad y el alcance que tienen las tecnologías que se utilizan. Solo si al vigilar las calles la policía retuviera y procesara toda la información sobre nuestras entradas, salidas, dirección, opiniones que damos en la calle o en centros comerciales, las personas con las que interactuamos, cosas que compartimos, tomara foto de nuestras formas de vestir y actividades, etc., se podría hacer la comparación entre patrullar la calle y el ciberpatrullaje, pero esto es imposible pues algo así no es tolerable en una sociedad democrática. (Fundación Karisma, 2023)

En consonancia con lo anterior, la CIDH identificó los problemas estructurales generados durante el Paro Nacional 2021, advirtiendo que las prácticas de ciberpatrullaje orientadas a un

monitoreo proactivo de contenidos presuntamente falsos sobre el desarrollo de protestas y la instigación del odio público, abrogarían facultades de chequeo de información y clasificación de contenidos, lo cual resulta preocupante pues categorizaría a ciudadanos, usando términos genéricos como “terrorismo” “vandalismo” y “criminales” y estigmatiza a las personas manifestantes. A su vez, la interrupción del servicio de internet en el contexto de las protestas, obstaculizó denuncias sobre el actúar de la fuerza pública. Al respecto menciona:

> La CIDH recomienda que estas restricciones de acceso a las redes, servicios y contenidos de Internet, tanto por medio del uso de tecnología con capacidad de alterar su acceso habitual, como por decisiones de restricción de acceso a contenidos, deben de estar previstas por una ley; perseguir un objetivo legítimo, necesario y estrictamente proporcional al fin que persiguen, así como estar sujetas al control judicial. (CIDH, 2021)

7.4.Tecnologías de utilización para la vigilancia

Como se mencionó anteriormente, una de las actividades desplegadas por la Policía corresponde al monitoreo del espectro electromagnético e interceptaciones de comunicaciones privadas sin autorización judicial previa, interfiriendo con la intimidad de la persona que envía y recibe información. No se exige que este procedimiento esté conforme al Código de Procedimiento Penal, ni tampoco la Ley de Inteligencia brinda protección contra las injerencias en comunicaciones privadas. El concepto utilizado en la norma conocida como Código de Policía tiene una definición estrecha de lo que se conoce como intimidad, confundiéndolo con derechos como el de libre desarrollo de la personalidad y la inviolabilidad del hogar.

Este marco teórico es importante en el sentido de la adquisición de tecnologías de vigilancia que operan fuera del ordenamiento jurídico, pues el decreto 1704 de 2012 no tiene

alguna disposición expresa que permita o prohíba esta vigilancia en masa. Algunas de las plataformas utilizadas son las siguientes:

1. *Plataforma única de monitoreo y análisis PUMA:* está relacionado con la infraestructura de red del proveedor de servicio, lo que potencialmente podría permitir la interceptación de comunicaciones de todas las personas que pasen por esta red, y dirija las instalaciones de monitoreo de las fuerzas de orden público.
2. *Sistema Integrado de Grabación Digital (SIGD):* Utilizado por la DIPOL (Dirección de Inteligencia Policial) es un sistema de vigilancia masiva, sin asistencia de proveedores del servicio.
3. *Sistema de control remoto (RCS)*[23]*:* Este es un sistema de intrusión adquirido por la policía en el 2015, usado para tomar el control de una computadora y dispositivos móviles sin ser detectado por el usuario, al "infectar" el dispositivo del blanco de vigilancia, pueden capturarse datos en el dispositivo del blanco, encender y apagar cámaras web, micrófonos, copiar archivos y contraseñas, como recoger, modificar y extraer datos del dispositivo objeto sin que sea detectado. A pesar de que la policía negó cualquier contrato de adquisición de este malware de la empresa Hacking Team, esta información es de información pública gracias a un documento filtrado donde se confirmó que sí querían activar este malware y utilizarlo (Privacy International, 2015)
4. *IMSI catcher:* Es un sistema de monitoreo móvil, que realiza interceptación al presentarse como una estación base a una red móvil, con la posibilidad de monitorear el funcionamiento del teléfono, llamadas, mensajes y ubicación en tiempo real. Este sistema

[23] Remote control system.

> fue adquirido a través de la empresa colombiana Microtel Ltda por la Dirección de Inteligencia Policial (DIPOL) desde el año 2005, y la Fiscalía y la DIJIN en 2014 ordenaron sistemas con esta tecnología invirtiendo una suma cercana de $280.000 dólares. (Privacy International, 2015)

Según la ONU la preocupación de sistemas de tecnología intrusiva no puede conciliarse con la legislación en vigor sobre vigilancia y acceso a la información privada, perturbando, el derecho a la intimidad, derechos a la equidad procesal pues estas pruebas pueden llegar a ser indicios en actuaciones judiciales. (UN. A/HRC/23/40, 17 de abril de 2013)

Por otro lado, los organismos que velan por la transparencia efectiva en los organismos de inteligencia no parecen tener claro en qué sentido pueden penetrar en este tipo de operaciones, pues la primacía del "orden público" crea un velo incuestionable sobre las actuaciones ejecutadas por Inteligencia.

Por lo tanto, es importante remarcar que el reconocimiento del derecho a la protección de datos personales frente a las agencias de inteligencia en fuentes abiertas y la obtención de información de la misma debe regularse, o al menos, recibir atención de autoridades de vigilancia, con posibilidad de extensión de mecanismos legales más claros en dichos asuntos; pues el hecho de que se traten publicaciones disponibles en internet pueden llegar a ser considerada información privada o sensible, a pesar de que se trate de escenarios diferentes a los habituados, el desvirtuar este espacio como propio forma parte de una de las discusiones más importantes en todo el mundo, por mencionar casos en China, Estados Unidos y Reino Unido. (Noujaim, Amer; 2019) . Este tema configura uno de los apartados del índice principal en el Curso elaborado desde la línea de tecnología, transparencia y DDHH, contextualizado e impartido dentro de la entidad; el

aprendizaje del mismo fue vital durante la práctica pues desde los últimos años se ha dado financiamiento a Dejusticia para trabajar temas de vigilancia e inteligencia estatal.

8. Brecha digital

Este último capítulo abordará la brecha digital existente en Colombia, lo que entendemos por la misma y qué implicaciones tiene para los derechos humanos. Al hablar de internet y la discusión principal de este trabajo, lleva consigo los presupuestos de que estamos conectados a la red, o que entendemos la interacción de la misma. No obstante, las desigualdades de acceso en el contexto colombiano siguen siendo imperantes, pues no se puede partir de la vulneración de derechos si de plano no se tiene capacidad para ejercerlos. La expresión de brecha digital, según Práxedes et al (2021) refiere al "diagnóstico y descripción de los efectos diferenciados, entre personas y grupos de personas, del despliegue de las tecnologías digitales en la sociedad" (pág. 29). No obstante, la definición se expande a las múltiples desigualdades existentes en el uso de tecnologías digitales, según Norris (2001) existen varios tipos de brecha digital, los cuales corresponden a:

1. **Brecha social:** diferencia entre el acceso a la información entre las personas de escasos recursos.
2. **Brecha global:** diferencia entre los países desarrollados y en desarrollo en el uso de TIC.
3. **Brecha democrática:** como la diferencia entre quienes utilizan las TIC para movilizarse y participar en la esfera pública.

A su vez, Jan Van Dijk propone una amplia explicación al fenómeno de brecha digital a partir de sus estudios que datan desde 2005. En un principio solo se mencionaba la brecha digital

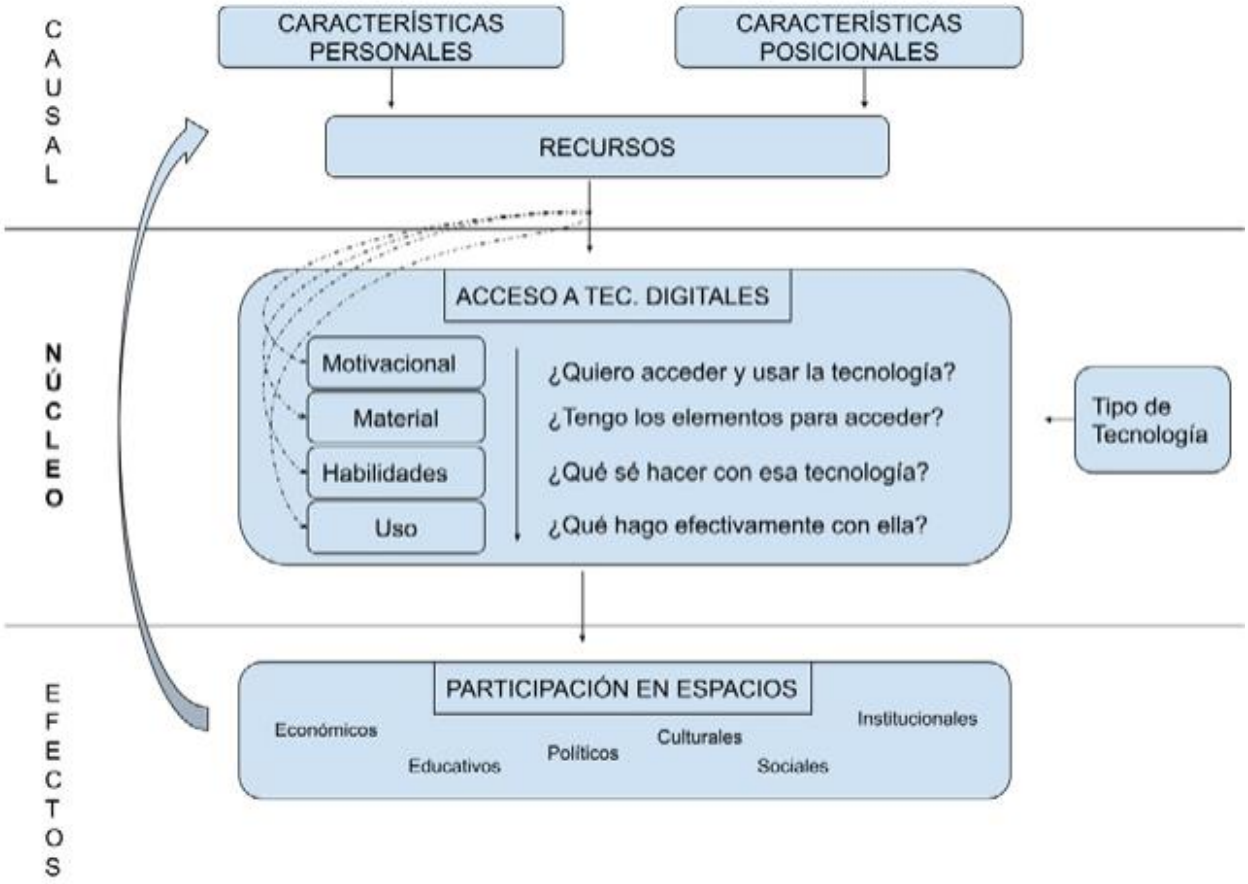
como los que poseían acceso a la tecnología y los que no, muy parecido a la definición que da el Ministerio de Tecnologías (MinTIC):

> La brecha digital hace referencia a la diferencia socioeconómica entre aquellas comunidades que tienen accesibilidad a las TIC y aquellas que no, y también hace referencia a las diferencias que hay entre grupos según su capacidad para utilizar las TIC de forma eficaz, debido a los distintos niveles de alfabetización y capacidad tecnológica. (MinTic, 2020)

No obstante, el modelo propuesto por Van Dijk (2005) parte de presupuestos personales, raciales, materiales e incluso culturales, como se muestra en el siguiente gráfico:

Figura 6.

Modelo de Van Dijk simplificado.



Nota: El gráfico representa un modelo simplificado de la teoría de acceso a redes propuesta por Van Dijk sobre las desigualdades en recursos que afectan el acceso a las tecnologías digitales. Tomado de Desigualdades digitales (p. 33), por Práexedes et al, 2021, Dejusticia ediciones.

El modelo de Van Dijk está divido en causales que causan que el acceso a tecnología sea difícil, se dividen en dos:

1. *Características de índole personal:* género, edad, grupo étnico racial y personalidades.
2. *Características posicionales:* educación, trabajo, tipo de hogar o geografía.

A su vez, las combinaciones de estas características determinan los recursos de la sociedad, los cuales pueden ser:

1. *Temporales:* tiempo disponible.
2. *Materiales:* ingreso y propiedades.
3. *Sociales:* relaciones humanas.
4. *Culturales o intelectuales*: conocimientos y habilidades.

Por lo tanto, el acceso a tecnologías de información (internet) está determinado por dichas características, que, a su vez, se pueden dividir en cuatro tipos de acceso que evolucionan de modo progresivo:

1. *Acceso motivacional:* inexistencia de voluntad de aprender a utilizar las tecnologías digitales. Puede darse por la percepción de que no se necesita o que no hay oportunidad para su acceso.
2. *Acceso material:* inexistencia de conectividad y a la disponibilidad de dispositivos, el mismo incluye las características de cobertura, calidad, puntos de acceso. También la capacidad de reemplazo de los dispositivos y costos de mantenimiento.
3. *Acceso a habilidades:* capacidad de las personas de adaptarse a tecnologías digitales, como básicas y operativas, y su aprovechamiento para lograr objetivos específicos.
4. *Acceso de uso:* posibilidad de hacer uso concreto de las tecnologías digitales, que se traduzca en una mayor y mejor participación en el ejercicio efectivo de los derechos. Ello se refleja también la capacidad de participar en diferentes espacios, como teletrabajo, e-learning, participar en asuntos públicos como presentar tutelas, o demandas. (Práexedes et al, 2021)

Por otro lado, la ONU ha realizado sus propios estudios al respecto, pues las tecnologías digitales parten de conformar la base para el cumplimiento de los objetivos de desarrollo sostenible; es por ello que proyectos como UN-Habitat buscan la conectividad de casi el 40% de la población restante por acceso a internet, denominando el objetivo como "inclusión digital":

> Hay muchas dimensiones de la brecha digital, que pueden variar desde físicas a psicológicas, el aumento de conectividad no es suficiente para resolver la brecha digital, la conectividad es un vehículo para aumentar el acceso a servicios públicos y a oportunidades para la ciudadanía. (ONU, 2021; pág. 17)

La relación de esta definición con los Objetivos de Desarrollo Sostenible, en concreto la meta 9, que pretende aumentar significativamente el acceso a la tecnología de la información y comunicaciones, tratando de proporcionar un acceso universal y asequible a Internet en los países menos adelantados (ONU, 2015). A su vez, en varias relatorías especiales se remarca la importancia del acceso a internet, según La Rue (2011):

> El acceso a Internet no solo es esencial para gozar del derecho a la libertad de expresión, sino también otros derechos, como el derecho a la educación, el derecho a la libertad de asociación y de reunión, el derecho a la plena participación en la vida social, cultural y política y el derecho al desarrollo social y económico (…) no solo [es] importante, sino imperativo que los Estados adopten políticas y estrategias efectivas y concretas … para que Internet esté ampliamente disponible y sea accesible y asequible para todos, basado en los principios de no discriminación de ningún tipo, incluso por motivos de raza, color, sexo, idioma, discapacidad, origen económico, o cualquier otra condición. (p. 19)

Las perspectivas de brecha digital pueden variar según distintos ángulos, según Van Dijk (2020) hay tres maneras de ver la brecha digital: innovación, inequidad y participación en la sociedad. La primera (innovación) consiste en adopción de tecnología de información y comunicación. La segunda concierne a la inequidad y refiere a las oportunidades que se tiene para obtener y usar tecnologías de información y comunicación. Por último, la de participación en la sociedad, referente a la inclusión o exclusión de una sociedad al adoptar y usar tecnología de información y comunicación (Van Dijk, 2020) Las formas de analizar la brecha digital muestran la complejidad de juridificar el acceso a internet, pues no solo deben tenerse en cuenta la conexión per sé, sino de alfabetización digital, disponibilidad de dispositivos, conectividad a nivel nacional, precios en tarifas de servicio, y políticas educativas en ciencia y tecnología. (Práexedes et al, 2021)

8.1. Brecha digital: perspectivas en Colombia

La visibilidad de las brechas digitales en Colombia se dio principalmente durante la pandemia de la COVID-19 en el año 2020. La dependencia a internet o tecnologías digitales se volvió fundamental, como una necesidad básica para -elementalmente- hacer cualquier tipo de trámite, proceso o ejercer derechos básicos como la educación, el trabajo, la justicia e incluso la salud. El tema ha sido trabajado en la institución Dejusticia, pues se visitan varias comunidades ubicadas sitios apartados como el Amazonas, la conexión con este tema deriva en la corrección, revisión y lectura de documentos concernientes a la brecha digital; este tema es uno de los focos principales del curso promovido por la Línea de Tecnología, transparencia y DDHH en el cuál se participó en su creación, y coordinación.

El concepto ya había sido analizado por el MinTic, con la ley 1978 de 2019, que modernizó la anterior ley 1341 de 2009, en el artículo 3° numeral 7:

> El derecho a la comunicación, la información y la educación y los servicios básicos de las TIC. En desarrollo de los artículos 16, 20 y 67 de la Constitución Política el Estado propiciará a todo colombiano el derecho al acceso a las tecnologías de la información y las comunicaciones básicas, que permitan el ejercicio pleno de los siguientes derechos: La libertad de expresión y de difundir su pensamiento y opiniones, el libre desarrollo de la personalidad, la de informar y recibir información veraz e imparcial, la educación y el acceso al conocimiento, a la ciencia, a la técnica, y a los demás bienes y valores de la cultura. Adicionalmente, el Estado establecerá programas para que la población pobre y vulnerable incluyendo a la población de 45 años en adelante, que no tengan ingresos fijos, así como la población rural, tengan acceso y uso a las plataformas de comunicación, en especial de Internet, así como la promoción de servicios TIC comunitarios, que permitan la contribución desde la ciudadanía y las comunidades al cierre de la ***brecha digital***, la remoción de barreras a los usos innovadores y la promoción de contenidos de interés público y de educación integral. La promoción del acceso a las tecnologías de la información y las comunicaciones básicas se hará con pleno respeto del libre desarrollo de las comunidades indígenas, afrocolombianas, palenqueras, raizales y Rrom. (Ley 1978 de 2019, artículo 3° numeral 7)

Según lo entiende la Corte Constitucional, el servicio de internet puede ser un medio para lograr progresivamente la plena efectividad de derechos como la educación (Corte Constitucional, T-030, 2020). Aunque los pronunciamientos de la Corte se han centrado más en la protección del derecho de la honra y el buen nombre, lo cierto es que su carácter fundamental en la vida diaria no está a discusión. Ello explica que la ONU haya declarado el acceso a la internet como derecho humano al igual que el Estado colombiano. (Ley 2180, 2021) (U.N, A/HRC/32/L.20)

Uno de los ejemplos más tratados por la jurisprudencia, es el acceso a la educación (remota), por otro lado, el caso judicial también se agudizó, con el decreto 806 de 2020, el acceso a la administración de justicia quedó relegado a la proporción de una conectividad estable, en cada línea de procesos, desde instaurar una demanda, hasta el proceso de cada una de las audiencias y trámites, para la realización de las audiencias -por ejemplo- se necesita de al menos una buena red de conexión a internet, que permita escuchar claramente al juez y a los demás convocados, y que también permita la participación de los demás de forma continua. La conexión a internet es solamente uno de los puntos que pueden bloquear el acceso a tener un proceso eficaz y diligente, y las intermitencias en el mismo pueden ocasionar incluso el efecto contrario a la garantía de un del acceso a justicia.

El análisis elaborado por Dejusticia en el libro "*Desigualdades Digitales: Aproximación sociojurídica al acceso a Internet en Colombia*" (2021) en las diferentes brechas digitales a partir del modelo de Van Dijk muestra las desigualdades de carácter personal y material; existe aún una gran parte de la población -especialmente, tercera edad- que no sabe cómo utilizar internet o por cuestiones motivacionales no decide usarlo. Otra de las razones principales corresponde al acceso material, el acceso a infraestructura, conectividad, costo de planes y equipos, representan obstáculos para las personas que quieren y necesitan acceder a internet.

Las diferentes perspectivas que se pueden tener sobre su uso también impactan los estudios de la brecha digital, en investigaciones sobre la Amazonía y su acceso a internet, las motivaciones de uso podrían ser diferentes a las tradicionales, al igual que los riesgos que puede implicar la tecnificación desde un enfoque étnico, según Ospina (2022): "[las comunidades]No ven internet como una herramienta para comunicarse que trae problemas, sino como una herramienta de reivindicación que les permite difundir y revitalizar su cultura ancestral" (p. 3). Si bien es cierto

que los fines son diferentes, la visión de internet como una necesidad es generalizada, sin embargo, las barreras geográficas y socioeconómicas impiden que esto suceda.

8.1.1. Ley 2108 de 2021.

La ley 2108 de 2021 o "*Ley de internet como servicio público esencial y universal*" tiene como objeto establecer dentro de los servicios públicos de telecomunicaciones, el acceso a internet como uno de carácter esencial, garantizando y asegurando la prestación del servicio de manera eficiente, continua y permanente, permitiendo -prima facie- la conectividad de todos los habitantes del territorio nacional, dando el mandato especial de la población que en razón a su condición social o étnica se encuentra en situación de vulnerabilidad en zonas rurales o apartadas (Ley 2180, 2021; art 1)

Su carácter orientador propende por las garantías mencionadas anteriormente: la **universalidad** de las TIC y masificación de uso de las TIC para el cierre de la brecha digital, teniendo en consideración a las personas que por razones sociales o étnicas se encuentren en situación de vulnerabilidad, junto con las que viven en condiciones de vulnerabilidad, o en zonas rurales, apartadas de difícil acceso. Dando un mandato claro las Instituciones que provean el servicio de acceso a internet, adoptando paquetes de medidas reglamentarias diferenciales y ofreciendo incentivos a las mismas para que garanticen la conexión efectiva de internet en las situaciones especiales anteriormente mencionadas.

Esta ley tiene consonancia con la ley 1341 de 2009, que declara en sus principios orientadores, algunos relacionados con la brecha digital de acceso a tecnologías en Colombia:

- *El uso eficiente de la infraestructura y de los recursos escasos*: por el cual el Estado fomentará el despliegue y uso eficiente de la infraestructura para la provisión de redes de

telecomunicaciones y los servicios que sobre ellas se puedan prestar, y promoverá el óptimo aprovechamiento de los recursos escasos con el ánimo de generar competencia, calidad y eficiencia, en beneficio de los usuarios, siempre y cuando se remunere dicha infraestructura a costos de oportunidad. Para tal efecto, dentro del ámbito de sus competencias, las entidades del orden nacional y territorial están obligadas a adoptar todas las medidas que sean necesarias para facilitar y garantizar el desarrollo de la infraestructura requerida, estableciendo las garantías y medidas necesarias que contribuyan en la prevención, cuidado y conservación para que no se deteriore el patrimonio público y el interés general. (Art 2, numeral 3)

- *El derecho a la comunicación, la información y la educación y los servicios básicos de las TIC:* El Estado proporcionará el acceso a tecnologías de la información y comunicaciones básicas, estableciendo programas para población pobre y vulnerable, población de 45 años en adelante y la población rural para el uso de plataformas y TIC de uso comunitarios, que permitan la *contribución desde la ciudadanía y las comunidades al cierre de la brecha digital*, la remoción de barreras a los usos innovadores y la promoción de contenidos de interés público y de educación integral. La promoción del acceso a las tecnologías de la información y las comunicaciones básicas se hará con pleno respeto del libre desarrollo de las comunidades indígenas, afrocolombianas, palenqueras, raizales y Rrom. (Art 2°, numeral 7)

A pesar de la referencia de Internet como un servicio público, las posiciones académicas / jurisprudenciales difieren pues aún hay facetas prestacionales de todos los derechos de contenido económico y social. La propuesta hecha por Práexedes et al (2021) corresponde a la visión del Internet como un derecho fundamental, partiendo de la base de que el internet es indispensable

para que toda persona (en Colombia) pueda concretar su plan de vida y pueda desarrollar un papel activo en la sociedad que habitamos hoy, creando una obligación en cabeza del Estado para avanzar de forma progresiva en generar condiciones para su goce tranquilo. Por último, la protección judicial de este derecho extendiendo la protección a mecanismos -ya utilizados- como la tutela u otros que se relacionen de forma directa con la prestación de este servicio.

9. Conclusiones

El ecosistema físico y cibernético en el que habitamos y nos desarrollamos hoy en día ciertamente ha cambiado, y con ello las costumbres de lo que se solía conocer como internet hace veinte años. El avance de la tecnología trae consigo el avance en preguntas de carácter social que juegan un importante papel en la protección de derechos humanos.

El objeto general de este trabajo de grado partió desde el análisis de las tecnologías de comunicación y redes sociales, relacionándolo con el impacto que las mismas tienen en los Derechos Humanos, específicamente en la vulneración de los mismos, partiendo desde la óptica trabajada desde la Línea de Tecnología, Transparencia y Derechos humanos en la institución de Dejusticia, los cuales incluyen la libertad de expresión, privacidad y acceso a la información. A pesar de ello, se concluye la importancia que tienen las mismas para materializar otros derechos como la libertad de expresión, la salud, el acceso a justicia, entre otros. Estamos permeados de forma constante por estas plataformas, por lo cual cuestionarse por su manejo en política de datos es una pregunta tanto válida como subversiva.

Continuando en la idea de que se trató de una práctica de investigación, la revisión de forma activa y sistemática de bibliografía propuesta en el marco de la práctica concerniente a temas de tecnología y derechos humanos contribuyó en gran parte al desarrollo y entendimiento de las

actividades propuestas de forma posterior dentro de la línea; el analizar los fenómenos digitales desde la óptica de la investigación permite abrir un campo más amplio para aportar ideas en su regulación, como el entendimiento de la vulneración de derechos en el ámbito internacional y nacional. Los temas que más relevancia cobraron durante el tiempo trabajado (y que forman parte de los objetivos propuestos dentro de la línea para el año 2023) correspondieron a libertad de expresión, moderación de contenido y desinformación; vigilancia estatal; y brecha digital. Dichos temas fueron trabajados en extenso, en especial para la preparación de cursos pedagógicos que tendrán una difusión de carácter interno en la institución, sin embargo, el aporte de bibliografía dejados en la base de datos de la institución, se espera, aporte una guía en los temas que se investigarán en un futuro dentro de Dejusticia.

En cuanto a la interpretación de las investigaciones realizadas, la vulneración sistemática de derechos humanos en este nuevo ámbito tecnológico constituye un reto para diferentes autores (Estado, Empresas, Ciudadanos), limitar derechos como la libertad de expresión por medio de moderación de contenidos amenaza seriamente la base democrática en un Estado de Derecho propendido por la Constitución.

Por otro lado, la garantía de privacidad por parte del Estado y las Empresas es un principio en desarrollo, el avance del reconocimiento del espacio digital como un espacio con protecciones materializables, cuyos derechos no son "*virtuales*" sino que pueden ser exigidos, eventualmente, ante la justicia, representan grandes cambios en la forma en cómo se percibe el derecho.

Las entidades públicas que velan por el cumplimiento de las leyes del ordenamiento colombiano o de Tratados Internacionales deben propender siempre por un estándar de transparencia, que se replique en todas las esferas que están bajo su control, el avance en la juridificación de prácticas como *ciberpatrullaje* o moderación de contenido son cuestiones que

están en constante avance, moldeándose a las situaciones de cada contexto; a pesar de que avance de forma exponencial, los retos de modernización exigen un constante aprendizaje y alfabetización entre la población, la comprensión de las mismas permitirá también el entendimiento de las responsabilidades que crea tanto para el Estado como para las Empresas de tecnologías.

En cuanto a la brecha digital existente -y que subsiste- en Colombia, los estudios realizados dentro de Dejusticia permiten ver este fenómeno como una de las tareas más importantes del Gobierno actual, a pesar de que los retos parezcan imposibles, la regulación para un espacio seguro y libre de amenazas se incrementa de forma exponencial por medio de jurisprudencia o legislación. El acceso a la información constituye un derecho, que ha sido reconocido incluso dentro de la misma legislación colombiana, si bien su materialización parece imposible, el propender por que el acceso al uso de tecnologías digitales y por ende, a información consignada en internet, es un deber Estatal de estricto cumplimiento en una sociedad *hiperconectada* como la actual.

Asimismo, cabe destacar que la alfabetización y puesta en conocimiento del uso consciente de las tecnologías permite revindicar los derechos humanos; aunque el espacio digital luzca como un gran espacio sin regulación específica, lo cierto es que la falta de la misma conlleva a que se vulneren los derechos anteriormente mencionados, por lo tanto, es importante reconocer que el espacio digital cobra -y cobrará- más fuerza con el tiempo, de ahí que, el enmarcar el uso de dichas tecnologías dentro de marcos constitucionales significa también proteger los derechos humanos.

Con respecto a las soluciones propuestas en el marco de la Línea en Dejusticia, se concluye el papel fundamental que juega la **transparencia**, pues la misma crea una consciencia ciudadana que propende por una mejor forma de ejercer sus derechos en un espacio -muchas veces- incierto y gaseoso como lo es el ciberespacio (internet). El hecho de que las instituciones públicas den la información de forma correcta, puede incrementar un proceso de democratización de la

información, sobre el contenido que consumismos, la utilización de nuestros datos personales y las implicaciones de privacidad que puede tener llegar a utilizarlas; el conocimiento sobre todo ello permite que tomemos decisiones de manera crítica y consciente, creando una ciudadanía mucho más democrática y autónoma sobre lo que consumimos -en contenido digital- diariamente.

Por último, los aportes dados por la práctica me permitieron expandir el conocimiento previo sobre tecnología, analizando no solo el punto de vista jurídico, sino el social; las diferentes perspectivas y verdades existentes detrás de todo lo que usamos cotidianamente (el ejemplo más representativo son las redes sociales) impactó de forma general en la manera en que percibo el contenido que consumo o busco en internet en estos momentos, a su vez, el entender dicha problemática desde el ámbito de vulneración de derechos como la libertad de expresión o privacidad proporciona un llamado de atención, tanto en las autoridades Estatales como en las Empresas de Tecnología cuyo crecimiento exponencial implica también un análisis consciente de las consecuencias e impactos en los derechos humanos, la responsabilidad existe y materializarla es un hecho que se construye entre cada uno de los individuos de la sociedad.

La importancia de analizar estos retos desde el punto de vista académico radica en los aportes que puede brindar la investigación, más aún, las investigaciones dadas por Dejusticia que conllevan componentes muy cercanos a la comunidad Colombiana e Internacional, el escuchar la voz de los propios actores permite que los fenómenos de vulneración de derechos sean reales y cercanos, al igual que la puesta en conocimiento público de cada uno de las investigaciones nos democratiza y autoriza como ciudadanos el conocer más sobre dichas vulneraciones en el ámbito tecnológico; el enfoque de “investigación-acción” provee una diferencia y dinamismo dentro de la Academia.

La posibilidad de abrir espacios donde se den a conocer estos temas significa un avance importante dentro y fuera de la institución; pues el tema de tecnología puede llegar a causar confusión debido a la cantidad de piezas técnicas y tecnológicas que están fuera de nuestro conocimiento general; por lo cuál la puesta en conocimiento de estos temas de forma más clara, concisa y alineada a los intereses de la Institución puede significar un avance importante para las investigaciones no solo de la línea de tecnología, sino de todas las líneas en general en Dejusticia; el trabajo que se hace en conjunto de otras organizaciones de carácter internacional demuestra la relevancia que tiene este tema en la actualidad, y el como comenzar por conocerlo puede conllevar a protegerlo.

La práctica -además de aumentar mis conocimientos- cambió mi perspectiva tanto de los problemas sociales como jurídicos, el instar la necesidad de regular y hablar sobre estos temas en otros espacios diferentes a mi ámbito de trabajo es una labor constante, que se puede articular en cualquier espacio, a pesar de que en este trabajo de grado se abordaron temas específicos, la línea de fenómenos tecnológicos e implicaciones para derechos humanos es bastante amplia, el situar una discusión que se esté actualizando constantemente me permitió ser mucho más crítica de los contenidos que se consumen o de los intentos que se dan por regularlo. El poner en evidencia dichos vacíos es solo el comienzo para crear un espacio más seguro y libre de vulneraciones; el hecho de que se tratase de una práctica de investigación también aportó en el ámbito de valorar la importancia y aporte de la academia, más aún, el de la formación que se da con respecto a dichos temas, pues del mismo se dan conjeturas diariamente, pero el estudiarlo desde una mirada más profunda implanta también la necesidad de enseñarlo tanto en las aulas escolares como en las universitarias, el articular planes de estudio que incluyan esta discusión permite que los conocimientos se actualicen y así poder ayudar en solucionar -o aportar- a los temas discutidos

anteriormente. El camino por recorrer implica muchos desafíos, empero, la responsabilidad por construir el mismo recae en cada uno de nosotros.

Referencias bibliográficas.

Ángel, M., Newman, V., Ospina, D. (2020). Rendición de cuentas de empresas con modelos de negocios basados en datos en Colombia: la protección de datos personales en la era digital. Dejusticia.

Amer, K., Noujaim, J. (Directores). (2019). The great hack. (Documental). Distribuido por Netflix.

Amaya, J., Zuluaga,S. (2022). El Régimen de Debida Diligencia Obligatoria: Estado del Arte e Implicaciones desde una Perspectiva Latinoamericana, Estudios en Derecho, Comercio & Globalización, Número 1. Universidad de los Andes. https://derecho.uniandes.edu.co/sites/default/files/el-regimen-de-debida-diligencia obligatoria.pdf.

Aritmetics (2023). Glosario: weareable. https://www.arimetrics.com/glosario-digital/wearable.

Botero, C. (12 de septiembre de 2020). Tenemos que hablar de la vigilancia digital estatal (primera parte). La silla vacía. https://www.lasillavacia.com/historias/historias-silla-llena/tenemos-que-hablar-de-la-vigilancia-digital-estatal-primera-parte-/

Camacho, L., Ospina, D., Upegui, J.C. (2023). Inteligencia estatal en internet y redes sociales: la privacidad bajo amenaza. Editorial Dejusticia. https://www.dejusticia.org/publication/inteligencia-estatal-en-internet-y-redes-sociales-la-privacidad-bajo-amenaza/.

Centeno, A. (2019). Deep learning. Trabajo de grado para optar al título de matemático. Universidad de Sevilla.

Claro, M., Santana, E., Alfaro, A., Franco, R. (2021). Ciudadanía digital en América Latina: revisión conceptual de iniciativas. Políticas Sociales, N° 239 (LC/TS.2021/125).

Cobo, P. (20 de abril de 2023). Cultura de cancelación. [Debate]. Feria Internacional del Libro (FilBo).

Colombia +20 (27 de mayo de 2023). Comisión de la Verdad entrega al país su archivo documental | Colombia +20. [Vídeo]. YouTube. https://youtu.be/uujXDipxKVc.

Corte Constitucional, Comunicado Sentencia SU-420, (M. P. José Fernando Reyes), Sep. 12/19.

Corte Constitucional. Sentencia T-063A de 2017, M. P. Jorge Iván Palacio Palacio; febrero 03 de 2017.

Corte Constitucional, T-203; 2022. M.P. Diana Fajardo Rivera: 9 de junio de dos mil veintidós 2022.

Corte Constitucional, T-729 de 2002. M.P. Eduardo Montealegre Lynett: 5 de septiembre de dos mil dos 2002.

Corte Constitucional, C-1140. MP. Manuel José Cepeda Espinosa, (31 de octubre de 2001).

Corte Constitucional, sentencias C-913 de 2010. M.P. Nilson Pinilla Pinilla: 16 de noviembre de dos mil diez 2010

Corte Constitucional. Sentencia T-280. MP. José Fernando Reyes Cuartas, (8) de agosto de dos mil veintidós (2022).

Corte Suprema de Justicia. Sala de casación penal. Sentencia STP9319-2020. MP: Eugenio Fernández Carlier; (27 Octubre 2020)

Comisión Internacional de Derechos Humanos (CIDH). (junio de 2021). Observaciones y recomendaciones, Visita de trabajo a Colombia. https://www.oas.org/es/cidh/informes/pdfs/ObservacionesVisita_cidh_Colombia_spA.pdf.

Comisión de la verdad. (2022). *La comisión*. https://web.comisiondelaverdad.co/la-comision/que-es-la-comision-de-la-verdad.

Cortés, C. (2020). La neutralidad de la red: la tensión entre la no discriminación y la gestión. *Internet y derechos humanos*. Bertorini.

CIDH. (18 de abril de 2020. *CIDH y su RELE expresan preocupación por las restricciones a la libertad de expresión y el acceso a la información en la respuesta de Estados a la pandemia del COVID-*

19. Comunicado de prensa R78/20. https://www.oas.org/es/cidh/expresion/showarticle.asp?artID=1173&lID=2.

Day, G., Schoemaker, P. (2001). Gerencia de Tecnologías Emergentes. 1ra edición. Editorial Javier Vergara.

Dias Oliva, T. (2020). Content moderation technologies: Applying human rights standards to protect freedom of expression [Tecnologías de moderación de contenido: aplicando derechos humanos a los estandares para proteger el derecho de libertad de expresión]. Human Rights Law Review, 20(4), 607-640.

de la Torre, I. (2018). La disrupción tecnológica ya está aquí: cómo afecta a las personas, los gobiernos y las empresas. Cuadernos de estrategia, (199), 25-68.

El estado monitorea internet: implicaciones en los derechos humanos del ciberpatrullaje. (19 de enero de 2023). Fundación Karisma. https://web.karisma.org.co/el-estado-monitorea-internet-implicaciones-en-los-derechos-humanos-del-ciberpatrullaje/.

Forero, F. (27 de abril de 2023). ¿Quién es el autor de las obras creadas por Inteligencia Artificial? Conferencia en el marco de la FilBo. Bogotá, Colombia.

FLIP (24 de agosto de 2021). Radicado GS-2021-108176-DIJIN-CECIP 1.10.

Informe del Relator Especial sobre la Promoción y Protección del Derecho a la Libertad de Opinión y Expresión, UN Doc. A/HRC/23/40, párr. 62 (17 de abril de 2013).

García, S., Gonza, A. (2007). La libertad de expresión en la jurisprudencia de la Corte Interamericana de Derechos Humanos. https://www.corteidh.or.cr/sitios/libros/todos/docs/libertad-expresion.pdf.

González, F. E. (2015). Nativos Digitales. Desafió de la educación actual. Paradígma, 31(2), 5-6.

Guinness, H. (2017). How Facebook's news feed sorting algorithm works. [Cómo funciona el algoritmo de clasificación de noticias de Facebook] Recuperado de: https://www.howtogeek.com/290919/how-facebooks-news-feedsorting-algorithm-works/

La Rue, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, [Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y de expression] 16 May 2011, A/HRC/17/27 at para 21.

Luján, S. (2012) Cookies: ¿Qué son y para qué sirven?. [Video]. Youtube. https://www.youtube.com/watch?v=8LaTgXMhgtE&t=1s.

Ley Estatutaria 1266 de 2018. Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones. Diciembre 31 de 2008. D.O. 47.219. http://www.secretariasenado.gov.co/senado/basedoc/ ley_1266_2008.html

Ley Estatutaria 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales. Octubre 18 de 2012. D.O. 48.587 http://www.secretariasenado.gov.co/senado/basedoc/ ley _1581_2012.html.

Ley 1712 de 2014. Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones. Marzo 06 de 2014. D.O. 49.084. http://www.secretariasenado.gov.co/senado/basedoc/ley_1712_2014.html.

Ley 1341 de 2009. Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones –TIC–, se crea la Agencia Nacional de Espectro y se dictan otras disposiciones. Julio 30 de 2009. D.O. 47.426.

Ley estatutaria 1621 de 2013. Por medio de la cual se expiden normas para fortalecer el Marco Jurídico que permite a los organismos que llevan a cabo actividades de inteligencia y contrainteligencia cumplir con su misión constitucional y legal, y se dictan otras disposiciones". Abril 17 de 2013. D.O. 48.764.

Hernández, N. (2018). Clasificación de los datos personales e implicaciones legales. Artículo elaborado para optar el título de abogada. Universidad Pontificia Bolivariana. Recuperado de: http://hdl.handle.net/20.500.11912/3595.

Mahesh, B. (2019). Machine Learning Algorithms -A Review.[Algoritmos de aprendizaje de máquinas – una revisión] 10.21275/ART20203995.

Martínez, M., Mora, C. (producción). (octubre de 2021). T1E6 Ciberpatrullaje: el nuevo juez de la verdad. Perifoneo: un pódcast sobre la libertad de expresión. https://open.spotify.com/episode/7cq0bUjyUJ5eNA91qaUAbr?si=d072d7491b3d4ceb.

Ministerio de Tecnología e Información (MINTIC). (2021). Sociedad de Información. https://mintic.gov.co/portal/inicio/Glosario/S/5305:Sociedad-de-la-Informacion.

Ministerio de defensa. (28 de abril – 27 de junio de 2021) Balance general - paro nacional 2021. https://www.mindefensa.gov.co/irj/go/km/docs/Mindefensa/Documentos/descargas/estudios_sectoriales/info_estadistica/InformeCorrido_Balance_Paro_2021.pdf.

Norris, P. (2001). Digital Divide, Civic Engagement, Information Poverty and the Internet Worldwide. [Brecha digital, compromiso cívico, pobreza informativa e Internet en el mundo] Cambridge: Cambridge University Press.

OEA. CIDH .Relatoría especial para la libertad de expresión. Declaración Conjunta Sobre Libertad De Expresión Y "Noticias Falsas" ("Fake News"), Desinformación Y Propaganda (Marzo 2, 2017)

Ortiz, R. (2001). *Habeas Data. Derecho Fundamental y Garantía de la Protección de los Derechos de la Personalidad*. Editorial Frónesis. Caracas Venezuela.

ONU: Asamblea General, Declaración Universal de Derechos Humanos, 10 diciembre 1948, 217 A (III), disponible en esta dirección: https://www.refworld.org.es/docid/47a080e32.html [Accesado el 18 Mayo 2023]

Práexedes, V., Ospina, D., Upegui, J., León, D. (2021). Desigualdades digitales: aproximación socio jurídica al acceso a internet en Colombia. Documentos 71. Editorial Dejusticia.

Pérez y Martínez (2022). Moderación privada de contenidos en Internet y su impacto en el periodismo. *OBSERVACOM*. https://www.observacom.org/moderacion-privada-de-contenidos-en-internet-y-su-impacto-en-el-periodismo/.

Privacy Internacional, Shadow State: Surveillance, Law and Order in Colombia, agosto de 2015. Disponible en: https://privacyinternational.org/report/991/shadow-state-surveillance-law-and-order-colombia

Privacy Internacional, Shadow State: Surveillance, Law and Order in Colombia [Estado en la sombra: Vigilancia, ley y orden en Colombia], Agosto de 2015, págs. 42. Disponible en: https://privacyinternational.org/report/991/shadow-state-surveillance-law-and-order-colombia.

Revista Semana (2020, mayo 1). Las carpetas secretas. *Semana*. https://www.semana.com/nacion/articulo/espionaje-del-ejercitonacional-las-carpetas-secretas-investigacion-semana/667616/

Riveros-Parra, M. A. (2022). Genocidio del siglo XXI: el caso de los rohingya. Oasis, (36), 203-224.

Romero, J. M. A. (2004). Ciberespacio y comunicación: nuevas formas de vertebración social en el siglo XXI. Espéculo*: Revista de Estudios Literarios, 27*, 31. Santiago, Comisión Económica para América Latina y el Caribe (CEPAL).

Rueda-López, J. (2007) La Tecnología En La Sociedad Del Siglo XXI: Albores De Una Nueva Revolución Industrial Aposta. *Revista de Ciencias Sociales*, núm. 32, enero-marzo, 2007, pp. 1-28. Luis Gómez Encinas ed. Móstoles, España.

Russo, L. (2001). Resisting Hyper-Digitalisation. Investigating Hybrid Practices in Contemporary Graphic Design [Resistiendo a la hiperdigitalización. Investigación de prácticas híbridas en el diseño gráfico contemporáneo]. Editorial Routledge Focus.

Saura García, Carlos. (2022). El lado oscuro de las GAFAM: monopolización de los datos y pérdida de privacidad. Veritas, (52), 9-27. https://dx.doi.org/10.4067/S0718-92732022000200009

Schneier, B. (2015). Data and Goliath: The hidden battles to collect your data and control your world. [Datos y Goliat: Las batallas ocultas para recopilar tus datos y controlar tu mundo]. WW Norton & Company.

T. Cormen, C. Leiserson, R. Rivest, C. Stein (2009). Introduction to Algorithm. [Introducción a los algoritmos] Cambridge: Mit Press.

UPR Report (octubre 2017). Informe de actor interesado Examen Periódico Universal 30° período de sesiones – Colombia. Presentado por Dejusticia, Fundación Karisma y Privacy International. https://privacyinternational.org/sites/default/files/2018-04/EPU_El%20derecho%20a%20la%20intimidad%20en%20Colombia_2017.pdf

Van Dijk, J. A. (2005). The deepening divide: Inequality in the information society [La division profundizada: inequidad en la Sociedad de información]. Sage publications.

Valtysson, B., Jørgensen, R. F., & Munkholm, J. L. (2021). Co-constitutive complexity: Unpacking Google's privacy policy and terms of service post-GDPR [Complejidad co-constitutiva: La política de privacidad y las condiciones de servicio de Google tras el RGPD]. Nordicom Review, 42(1), 124–140. **https://doi.org/10.2478/nor-2021-0033**.

Weinberger, D. (2019). Everyday chaos: Technology, complexity, and how we're thriving in a new world of possibility.[El caos cotidiano: Tecnología, complejidad y cómo prosperamos en un nuevo mundo de posibilidades] Harvard Business Press.

Zuboff, S. (2020). Capitalismo de la vigilancia. Harvard University Press.