Terrorismo Digital en Colombia:

Un análisis desde el Derecho Penal del Enemigo, 2020-2025.

Autor:

Karol Valentina Chaves Prieto

Universidad Colegio Mayor de Cundinamarca

Programa Maestría en Derecho Penal

2025

Bogotá 2025.

Terrorismo Digital en Colombia:
Un análisis desde el derecho penal del enemigo, 2020 - 2025.

Karol Valentina Chaves Prieto

Trabajo de Grado presentado como requisito para optar al título de Maestría en Derecho Penal

Director (a) Temático: Claudia Patricia Orduz Barreto.
Director (a) Metodológico: Myriam Sepúlveda López.

Línea de investigación 02.

Universidad Colegio Mayor de Cundinamarca

Programa Maestría en Derecho Penal

2025

Nota de aceptación

Asesora Temática:

Dra. Claudia Patricia Orduz Barreto.

Asesora Metodológica:

Dra. Myriam Sepúlveda López

Jurado 1:

Yaneth Osana Gonzalez Chacón

Jurado 2:

Dr. Jaime Alfonso Cubides Cárdenas

5 de diciembre del 2025

Dedicatoria y Agradecimientos

Este trabajo está dedicado, con todo mi cariño, a todas las personas que han hecho parte de este camino y que de una u otra forma me ayudaron a llegar hasta aquí.

A mi familia, por estar conmigo siempre, apoyándome sin dudar, caminando a mi lado; creyendo en mí en cada paso, hemos logrado tantas cosas juntos, cada una de ellas tiene un pedacito de su amor incondicional.

A mi padre, a mi madre, a mis hermanos y a mi abuela: este logro es para ustedes y por ustedes, no esperen menos de mí, porque todo lo que hago, lo hago con amor. Los amo con todo mi corazón.

A mi gatito, que aunque no pude dedicarle tanto tiempo como hubiera querido, siempre fue mi compañía silenciosa y paciente. A veces sacrificamos momentos de juego o cariño por este proceso, pero su amor constante me recordó la importancia de las pequeñas pausas y del afecto sincero. Lo amo profundamente, este logro también es para él, que me esperó con la misma ternura de siempre.

A mis amigos, que siempre estuvieron ahí para mí, apoyándome, celebrando mis avances y acompañándome en los momentos difíciles. Gracias por estar presentes, por quererme tanto; por hacer de cada proyecto una aventura compartida. Tenerlos conmigo ha sido una de las mayores bendiciones de mi vida.

A mis asesoras, la Dra. Claudia y la Dra Myriam, gracias por su apoyo incondicional, por su orientación constante, por sus observaciones tan valiosas. En los momentos en que sentía que no podía más, sus palabras y su confianza me ayudaron a seguir adelante. Gracias por su trato cálido, por estar ahí siempre.

A mis profesores de metodología, el Dr. Flover y al Dr Cubides, gracias por haberme enseñado a construir una investigación sólida y rigurosa, sus clases me permitieron desarrollar este trabajo con una base firme y con un enfoque investigativo claro.

Al Dr. Sergio, gracias por ayudarme a entender una doctrina que en su momento me parecía tan compleja, por enseñarme a mirar más allá de los sesgos, con pensamiento crítico y apertura.

A mi alma mater, la Universidad Colegio Mayor de Cundinamarca, por ser el lugar donde crecí, aprendí y me formé, no solo académicamente, sino también como persona.

Gracias por permitirme vivir un proceso tan completo, desde el pregrado, la especialización y ahora la maestría.

Gracias por ser una universidad pública de excelente calidad, por haberme brindado la oportunidad de ser becada y seguir construyendo mi camino profesional en sus aulas.

A todos y cada uno de ustedes, gracias.

Con amor, con gratitud y con un corazón lleno de emoción, les dedico esta tesis.

Porque cada palabra, cada idea y cada logro que aquí se escribe, también les pertenece…

Lista de Tablas.

Lista de Figuras

Lista de Anexos

Anexo 1. Matriz denominada “Matriz de Aplicación de la Teoría del Derecho Penal del Enemigo (TDPE)”, junto con sus instrucciones de uso y aplicabilidad en los documentos CONPES 3995 de 2020 y CONPES 4144 de 2025.

Anexo 2. Pieza publicitaria, Programa Radial de la Universidad Colegio Mayor de Cundinamarca sobre el Terrorismo Digital en Colombia.

Anexo 3. Artículo titulado “El Terrorismo Digital en Colombia: entre el Derecho Penal del Enemigo y el Estado Social de Derecho ” resultado de la reflexión académica derivada del proyecto de investigación, en conjunto con su constancia de envió a la revista académica.

Anexo 4. Constancia de Clases Magistrales expedido por la Facultad de Derecho, Universidad Colegio Mayor de Cundinamarca.

Anexo 5. Constancia de Entrega y Guía del Derecho Penal del Enemigo al Consultorio Jurídico de la Universidad Colegio Mayor de Cundinamarca.

Anexo 6. Constancia de Ponencia en Seminario De Actualización En Reforma Al Código Penal el 13 de Noviembre de 2025. Tema: “El Terrorismo Digital desde la perspectiva del Derecho Penal del Enemigo”

Anexo 7. Proyecto de Ley “Por medio de la cual se reconoce el uso de medios digitales como modalidad agravada del terrorismo y se modifica el artículo 344 del Código Penal colombiano.”

Resumen

La presente investigación analiza el tratamiento jurídico-penal del Terrorismo Digital en Colombia entre 2020 a 2025, a la luz de los fundamentos del Derecho Penal del Enemigo formulado por Günther Jakobs; con el propósito de determinar si la respuesta estatal frente a las amenazas del Ciberespacio ha mantenido su anclaje en el Estado Social de Derecho o si ha derivado hacia un modelo punitivo de excepción. El estudio parte de la comprensión del impacto de las transformaciones tecnológicas sobre el Derecho Penal y de cómo el terrorismo ha trasladado su escenario de acción al entorno digital, aprovechando la desregulación y la expansión del uso de internet, especialmente tras la pandemia de la COVID-19.

En este marco, la investigación tiene como propósito delimitar el concepto de Terrorismo Digital, sistematizar los fundamentos del Derecho Penal del Enemigo, analizar el tratamiento jurídico-penal colombiano mediante una matriz aplicada a los documentos CONPES 3995 de 2020 y 4144 de 2025 y formular propuestas sociojurídicas que aseguren la protección efectiva de los derechos fundamentales. Los hallazgos permiten identificar una tendencia estatal orientada a la prevención, la cooperación institucional y la gestión del riesgo, más que a la adopción de un modelo penal de exclusión, lo cual abre un espacio de reflexión sobre el equilibrio entre seguridad digital y principios constitucionales en el Estado Social de Derecho.

Palabras Clave: Terrorismo Digital (TDig), Derecho Penal del Enemigo, Estado Social de Derecho, Seguridad Digital y Ciberespacio.

Abstract

This research analyzes the legal and criminal treatment of digital terrorism in Colombia between 2020 to 2025, in light of the foundations of Enemy Criminal Law (TDPE) formulated by Günther Jakobs, with the aim of determining whether the state's response to cyberspace threats has remained anchored in the Social Rule of Law or has shifted toward an exceptional punitive model. The study begins with an understanding of the impact of technological transformations on criminal law and of how terrorism has shifted its arena of action to the digital environment, taking advantage of deregulation and the expansion of internet use, especially since the COVID-19 pandemic.

In this framework, the research aims to delimit the concept of digital terrorism, systematize the foundations of the Criminal Law of the Enemy, analyze the Colombian criminal-legal treatment through a matrix applied to CONPES documents 3995 of 2020 and 4144 of 2025, and formulate socio-legal proposals that ensure the effective protection of fundamental rights. The findings make it possible to identify a state trend oriented toward prevention, institutional cooperation, and risk management, rather than the adoption of an exclusionary criminal model, which opens a space for reflection on the balance between digital security and constitutional principles within the Social Rule of Law State.

Keywords: Digital terrorism, enemy criminal law, social rule of law, digital security, and cyberspace.

Tabla de Contenido

Lista de siglas y abreviaturas

Sigla	Significado
TDig	Terrorismo Digital (TDig)
TDPE	Teoría del Derecho Penal del Enemigo
ESD	Estado Social de Derecho (ESD)
IA	Inteligencia Artificial
TIC	Tecnologías de la Información y Comunicación

Introducción

Con el desarrollo tecnológico, la sociedad ha evolucionado de manera significativa transformando las dinámicas que de ella se desprenden, particularmente, al generar nuevos espacios de conexión no físicos, como lo es el Ciberespacio donde se ha concentrado el uso exponencial de la Tecnologías Dedicadas a la Información y/o Comunicación, también llamadas (TIC), convirtiéndose tanto en una oportunidad de avance, como una nueva amenaza que desafía los marcos jurídicos tradicionales bajo un mundo dirigido por alcances globalizados.

En este contexto, las nuevas tecnologías informáticas que procesan de manera eficiente grandes cantidades de información, han sido acaparadas por personas dispuestas actuar en contra de los propios fines de la población, facilitando y mutando la comisión de conductas punibles de manera inclemente, siendo previsible la respuesta punitiva del Estado.

En verbigracia, el terrorismo como figura tradicional de violencia, que parte como actuación criminal en contra de los intereses de la sociedad ha descubierto en estos espacios virtuales poco regularizados, una forma eficaz de ejercer su actividad, obteniendo provecho al rol emergente de la tecnología para la masterización de sus actos.

Colombia, no ha sido indiferente a esta tendencia, la seguridad digital para el territorio se ha convertido en un objetivo trascendental; dado a las lagunas jurídicas que han surgido frente a la rápida evolución del Ciberespacio que actores terroristas han sabido aprovechar, intensificando sus operaciones a partir de la pandemia de COVID 19, al existir una mayor dependencia a la tecnología.

Razón por la cual, se hace necesario observar si la respuesta punitiva del Estado a esta reciente amenaza ha generado un tratamiento diferente al penal clásico, e incluso si ha incorporado elementos de la Teoría del Derecho Penal del enemigo(TDPE) desarrollada por Gunter Jakobs y de ser así cuáles serían sus implicaciones en un Estado Social de Derecho (ESD).

Por ello se pretende analizar de qué manera se ha desarrollado el Terrorismo Digital (TDig) en Colombia en relación con los fundamentos teóricos del Derecho Penal del Enemigo (DPE) de Günter Jakobs entre 2020 a 2025; partiendo de la posibilidad de que el Estado Colombiano frente al Terrorismo Digital (TDig) se encuentre incorporando —de manera implícita o parcial— los postulados de este derecho excepcional.

Para comenzar tan digna travesía, se hace menester destacar, que el presente trabajo de investigación se encontrará desarrollado en tres capítulos a seguir:

En primer lugar conceptualizará el Terrorismo Digital (TDig) a partir de sus dimensiones históricas, tecnológicas, normativas y políticas; en segundo lugar se sistematizará los principios del Derecho Penal del Enemigo(DPE) propuesto por Günter Jakobs mediante la elaboración de una matriz analítica, permitiendo identificar sus rasgos distintivos y criterios verificables.

En tercer lugar, se examinará el tratamiento jurídico-penal del Terrorismo Digital (TDig) en Colombia entre 2020 a 2025 aplicando la matriz del TDPE, identificando la presencia de sus postulados en los documentos CONPES 3995 de 2020 y 4144 de 2025; por último, se propondrá estrategias que garanticen el respeto a los principios de un Estado Social de Derecho (ESD) frente al tratamiento jurídico-penal del Terrorismo Digital (TDig).

Finalmente, la investigación presenta estrategias de tipo socio jurídico y pedagógicas que favorecen la consolidación de la capacidad institucional del Estado Social de Derecho (ESD) sin comprometer sus principios constitucionales, garantizando un equilibrio entre la seguridad digital y la protección de los derechos fundamentales.

En suma, la investigación persigue ofrecer una lectura crítica y propositiva acerca de la mutación del poder punitivo en la era digital, visibilizando los retos que el Terrorismo Digital (TDig) impone a la vigencia de la juridicidad y a la salvaguarda de los valores democráticos**.**

1. Ubicación del problema.

1.1. Descripción del Problema

Uno de los debates más cuestionados dentro de la academia jurídica en la posmodernidad, es el fenómeno tecnológico, que ha desencadenado a finales del siglo XX e inicios del siglo XXI, una serie de implicaciones en el ámbito del derecho. Considerando, su gran impacto en la sociedad, dando lugar a la creación de complejas dialécticas de intercomunicación, generando tensiones que desbordan previsiones normativas.

Esto se traduce, en la aparición de nuevas formas de criminalidad que, al ser transaccionales y basarse en infraestructuras digitales, representan retos de gran envergadura frente a los marcos jurídicos tradicionales.

Como muestra de ello, la figura del terrorismo, ha encontrado en las nuevas tecnologías un espacio óptimo para el desarrollo de sus actividades ilícitas, siendo una herramienta que lo potencia y perfecciona; logrando mayor efectividad en su operación, convirtiéndolo en un fenómeno difícil de combatir para el Estado, por su capacidad de adaptación en nuevos espacios.

Es así como, los nuevos escenarios tecnológicos han agudizado irrevocablemente la evolución de actos terroristas en espacios virtuales escasamente regulados, en particular en plataformas digitales, flujos de información, entre otros espacios de la gran red (internet) difundiendo información, propaganda, reclutando seguidores, coordinando operación, entre otros, con la finalidad de desestabilizar el orden público.

Si bien, su fortalecimiento ha ido en ascenso, desafiando las estructuras tradicionales del Derecho Penal, es con la pandemia del COVID-19, que se amplió significativamente el alcance de las plataformas virtuales a nivel mundial.

Según la Unión Internacional de Telecomunicaciones (ITU, 2021, citado en Fundación Paz & Reconciliación- Pares, 2022), el impacto de la crisis sanitaria ha transformado la dependencia de los servicios digitales, al disponer:

> (…) el impacto que la pandemia tuvo sobre la forma como la sociedad opera, generó un incremento significativo en el tráfico de información en internet y los medios de comunicación. Por tanto, es necesario que los Estados adopten legislaciones y políticas que incentiven un Ciberespacio seguro y que permita que las personas sigan conectadas (p. 3).

De allí que, la crisis sanitaria trajo consigo la consolidación y precipitación de la virtualidad en todas las esferas sociales "un cambio que venía produciéndose desde hace tiempo, como es el traslado de algunas actividades del espacio físico al Ciberespacio"(Llinares, 2021, p. 3), pero que es a través de la pandemia que pudo materializarse en su totalidad.

Con ello, el impacto de la crisis generó una elevación en el tráfico de la información y una dependencia total de los servicios digitales a nivel global, incrementando a su vez la exposición de los particulares y Estados a nuevos riesgos cibernéticos.

Tabla 1.

Proporción de personas que utilizan internet en 2023.

DEPARTAMENTO	Total nacional (%)	Cabecera (%)	Centros poblados y rural disperso (%)
Total nacional	**77,3**	**82,6**	**59,6**
Amazonas	39,3	49,6	28,0
Antioquia	80,9	83,7	68,7
Arauca	66,0	78,1	42,9
Atlántico	80,6	81,3	68,0
Bogotá, D.C.	85,9	85,9	78,4
Bolívar	69,2	74,8	53,6
Boyacá	67,9	76,6	54,1
Caldas	76,6	81,7	59,0
Caquetá	72,3	74,7	67,5
Casanare	75,8	83,0	56,4
Cauca	65,9	79,5	58,2
Cesar	75,0	79,6	60,6
Chocó	43,4	66,2	25,7
Córdoba	67,5	77,0	57,1
Cundinamarca	83,5	86,2	74,6
Guainía	53,6	68,3	40,0
Guaviare	71,8	78,8	62,3
Huila	77,5	81,5	71,5
La Guajira	52,6	71,2	33,4
Magdalena	72,1	77,3	60,5
Meta	86,7	89,4	78,2
Nariño	66,0	77,8	56,6
Norte de Santander	74,4	78,7	57,2
Putumayo	59,4	71,6	45,7
Quindío	80,6	81,5	73,6
Risaralda	78,5	82,9	60,2
San Andrés	68,8	68,8	*
Santander	80,9	87,1	58,8
Sucre	66,8	76,1	51,7
Tolima	76,2	81,5	63,9
Valle del Cauca	84,7	86,1	76,1
Vaupés	34,1	66,4	20,5
Vichada	14,5	51,1	2,7

Fuente: Tomada del Departamento Administrativo Nacional de Estadística, 2023, Encuesta de Calidad de Vida- ECV (p.12)

En el caso colombiano, este incremento se deja ver con claridad ya que en 2023 “un 77,3% de las personas de cinco años y más usó Internet (82,6% en cabeceras y 59,6% en zonas rurales), mientras que en 2022 el total se situó en 72,8% (78,9% en cabeceras y un 52,6% en centros poblados y rural disperso” (DANE, 2023, p.13).

Estas cifras evidencian un incremento sostenido en el despliegue digital, a la vez que amplía los ámbitos de acción potencial de las estructuras ilícitas en el Ciberespacio, aumentando los desafíos del Estado en lo que toca a la prevención, control y regulación de actividades terroristas en línea.

Ante este contexto, el Terrorismo Digital (TDig) se presenta como una amenaza latente para el sistema social, acelerado por una pandemia; que en particular, compromete la estabilidad

del orden social y la seguridad nacional al generar miedo y zozobra en la población en el Ciberespacio y comprometiendo la integridad informacional de las instituciones de los Estados.

Frente a ello, surge la necesidad de abordar como el Estado ha fortalecido su respuesta, frente a este problema y si en su camino ha endurecido la legislación penal o ha generado estrategias públicas de persecución digital como los documentos CONPES 3995 de 2020 y 4144 de 2025.

En verbigracia, el Documento CONPES 3995 de 2020, que define la "*Política Nacional de Seguridad Digital*", advierte que "Las amenazas, los ataques e incidentes de seguridad digital cada día son más sofisticados y complejos e implican graves consecuencias de tipo económico o social." (Consejo Nacional de Política Económica y Social, 2020, p.3).

Asimismo el CONPES 4144 de 2025, correspondiente a la *"Política Nacional de Inteligencia Artificial"* establece que frente al uso malintencionado de la IA puede conducir a la desinformación entendida como" información falsa o imprecisa que intenta engañar y que es compartida a través de medios digitales con la intención de hacer daño y puede ser presentada en diferentes formas incluyendo textos, imágenes o videos*"* (Consejo Nacional de Política Económica y Social, 2025, p.38).

Así, se pone en consideración reflexionar si las medidas contenidas en tales políticas encauzadas a garantizar la seguridad digital y evitar el riesgo indeseable de los riesgos tecnológicos acaban por introducir una perspectiva de control que, inevitablemente, reemplace el Derecho Penal tradicional.

Continuando con este razonamiento, la expansión del aparato punitivo en las esferas del Ciberespacio, junto a la retórica de la seguridad, puede suponer, por el contrario, un tránsito del Derecho Penal garantista a un Derecho Penal preventivo y de excepción, donde el sospechoso ciudadano se convierte en "enemigo" incluso antes de haber perpetrado una conducta punible.

De esta manera, el eje central del estudio consiste en averiguar si el tratamiento del Terrorismo Digital (TDig) en Colombia (de manera temporal, entre el 2020 y el 2025) se aferra a

un modelo de Derecho Penal de enemigo que pone por delante la seguridad del ejercicio estatal frente a los derechos individuales; o bien, por el contrario, si continúa en su anclaje a los valores del Estado Social de Derecho (ESD), sustentados por la dignidad humana.

Por consiguiente, se establece la siguiente pregunta de investigación:

1.2. Formulación del Problema.

¿De qué manera se ha desarrollado el Terrorismo Digital en Colombia en relación con los fundamentos teóricos del Derecho Penal del Enemigo de Günter Jakobs entre 2020 a 2025?

1.3. Justificación.

En la última década, el Terrorismo Digital (TDig) ha emergido como una amenaza creciente en Colombia, experimentando un notable auge a partir de la pandemia de COVID-19, planteando desafíos sin precedentes para la seguridad nacional, lo cual, ha sido objeto de análisis por parte de organismos internacionales.

El Instituto de Investigación Interregional sobre Crimen y Justicia de las Naciones Unidas (UNICRI), en su informe de 2020, ha destacado:

> La desinformación y la información errónea en las redes sociales no son problemas nuevos, pero la crisis de la COVID-19 los ha amplificado y ha creado nuevas oportunidades para actores no estatales violentos. En los últimos meses hemos visto numerosos casos de uso malintencionado de las redes sociales, para socavar la confianza en los gobiernos y, al mismo tiempo, reforzar las narrativas extremistas y las estrategias de reclutamiento. (p.5).

En igual sentido, Jürgen Stock, Secretario General de INTERPOL señaló que “esta coyuntura especial ha sido aprovechada por los grupos cibercriminales para acelerar sus campañas

de dispersión de malware, el compromiso de data sensible en las organizaciones, facilitar las estafas en Internet y la desinformación" (Bautista, 2020, p. 4)

A nivel nacional, el periódico el Espectador (2025) en su artículo establece que más del 78% ha sido víctima de amenazas digitales entre las principales se encuentran:

> (…) la desinformación (59 %), la exposición a contenidos violentos (47 %) y el discurso de odio (39 %). Además, el estudio alerta sobre un fenómeno preocupante: la creación de deepfakes de contenido pornográfico, una práctica que afecta al 20 % de los encuestados en Colombia, posicionando como el segundo país con mayor incidencia de este problema.

Estos datos reflejan, que los grupos terroristas han evolucionado para adaptarse a esta nueva era representando una mayor amenaza estatal en el anonimato, incitando la violencia, coordinando ataques, difundiendo discursos que afectan a la seguridad del Estado y sus ciudadanos, lo cual, demanda una respuesta eficaz ante las vulnerabilidades del ecosistema virtual.

Generalmente, la respuesta punitiva contempla nuevos desafíos dentro del marco del Derecho Penal tradicional, en la medida que su alcance puede resultar ineficiente ante la amenaza significativa que trasciende el cerco de criminalidad común y se concentra en un dominio artificial no físico.

En este escenario de la era digital, los Estados redefinen el concepto de seguridad tradicional, a un modelo de seguridad tecnológico y de riesgo, en el que la protección del orden social y de las informaciones en un pilar del poder estatal.

No obstante, como advierte Mendoza Buergo (2001),cuando Derecho Penal se orienta en función de control preventivo de un riesgo, se corre el peligro de convertir al ciudadano en objeto de la neutralización, alterando la balanza entre libertad y seguridad.

Por lo tanto, la Teoría del Derecho Penal del Enemigo (TDPE) tiene un sentido en la medida que ofrece una conceptualización que permite verificar si la contestación estatal frente al

Terrorismo Digital (TDig) se ajusta a un modelo de gestión del riesgo o a uno de neutralización del peligro, que amenaza los principios del Estado Social de Derecho (ESD).

Razón por la cual, la Teoría del Derecho Penal del Enemigo (TDPE) cumple con el papel de lente crítico, que permite examinar o escrutar si las políticas y normas que se adoptan respetan los límites constitucionales consentidos para el poder punitivo.

Bajo estos parámetros, la relevancia de esta investigación radica, precisamente, en la necesidad de determinar si el Terrorismo Digital (TDig) en Colombia configura un escenario propicio para la aplicación de la Teoría del Derecho Penal del Enemigo (TDPE) y cuáles serían sus consecuencias en términos de derechos fundamentales y garantías procesales; lo cual, supone un análisis crucial para comprender los alcances del Derecho Penal frente así su aplicación es compatible al ordenamiento jurídico colombiano.

Desde un enfoque teórico y práctico, este estudio contribuirá al debate jurídico sobre el equilibrio entre seguridad pública versus garantías individuales, proporcionando herramientas para la formulación de estrategias que mitiguen las implicaciones de la Teoría del Derecho Penal del Enemigo (TDPE) en la lucha contra el Terrorismo Digital (TDig); así, se buscará fortalecer la capacidad del Estado para abordar esta amenaza sin comprometer los valores esenciales de un sistema garantista.

En conclusión, resulta significativo y necesario este trabajo al examinar un fenómeno jurídico como el Terrorismo Digital (TDig) inexplorado desde una óptica crítica, interdisciplinaria y constitucional, con la que se puede aportar claridad sobre los problemas que presenta el Estado colombiano frente a la criminalidad digital.

En definitiva, la investigación tiene por objeto ultimo contribuir al fortalecimiento de un modelo de Derecho Penal garantista, contra la lucha contra el Terrorismo Digital (TDig), el cual debe ser desarrollado dentro del ordenamiento jurídico y no al margen de este.

1.4. Objetivos

1.4.1. Objetivo General.

Analizar de qué manera se ha desarrollado el Terrorismo Digital en Colombia en relación con los fundamentos teóricos del Derecho Penal del Enemigo de Günter Jakobs entre 2020 a 2025.

1.4.2. Objetivos Específicos.

- Delimitar el concepto de Terrorismo Digital a partir de sus dimensiones históricas, tecnológicas, normativas y políticas, con el fin de precisar su alcance dentro del contexto de la seguridad digital en Colombia.

- Sistematizar los principios del Derecho Penal del Enemigo propuesto por Günter Jakobs mediante la elaboración de una matriz analítica, permitiendo identificar sus rasgos distintivos y criterios verificables.

- Examinar el tratamiento jurídico-penal del Terrorismo Digital en Colombia entre 2020 a 2025 aplicando la matriz del TDPE.

- Proponer alternativas de intervención socio jurídicas que garanticen el respeto a los principios de un Estado Social de Derecho frente al tratamiento jurídico-penal del Terrorismo Digital.

2. Marco Teórico

2.1. Capítulo I. El Terrorismo Digital: Un Estudio Multidimensional desde las Perspectiva Histórica, Filosófica, Jurídica y Político-Normativa.

2.1.1. Fundamentos del Estado ante el Terrorismo: El Contractualismo, la Seguridad Pública y el Derecho a Resistir.

El Estado es una construcción histórica, una estructura mutable que cambia conforme a las necesidades sociales de quienes la erigen; de allí, que no sea un ente espontáneo sino un producto de la historia de la humanidad para regular su desarrollo en sociedad. Su propia legitimidad, depende de la delegación de prerrogativas y libertades de los individuos, en aras de mantener el orden.

Es en la modernidad que está institución se conforma en su totalidad, a partir de dos perspectivas filosóficas; en primer lugar como estado hobbesiano dirigido a un absolutismo que buscaba un paulatino acaparamiento del poder coercitivo en la figura del monarca y; en segundo lugar, como contraposición, el estado nación desde la perspectiva burguesa o libertaria enfocada hacia un sistema capitalista y garantista de derechos individuales.

Conforme a este planteamiento, la implementación de una ficción como lo es el Estado, cimentada en la adhesión de múltiples voluntades de particulares que buscan un fin en común; logra que esta figura se vuelva una divinidad jurídica, con las características que le son propias: como la omnipotencia, omnipresencia e incluso la inmortalidad; interactuando con las personas, sin que el individuo pierda su autonomía o se difumine en la estatalidad.

Dicha institucionalidad logra, la erradicación de la anarquía y el enfoque de un poder político común donde “el Estado pasará a ser el único juez posible y el único verdugo habilitado para determinar la forma en la que se habrá de buscar la paz y habrá de respetar la igualdad y la seguridad”(Gialdino, 2018, p. 90).

Desde esta perspectiva se identifica un rasgo característico de la naturaleza misma del Estado, la cual es la preocupación por la seguridad pública, lo que justifica no sólo su creación, sino que se torna en un pilar fundamental en la consolidación del Estado Moderno y que le permite ejercer el monopolio de la fuerza.

Ahora bien, el contractualismo exhibe como punto de partida la categoría de un estado naturaleza que empieza a forjar ese rasgo característico; lo anterior, debido a que la condición hipotética de seres humanos actuando conformé a su libre albedrío, se convierte por excelencia en la justificación del pacto social, al examinar el impulso de los seres humanos en forjar una sociedad civilizada.

Desde una exploración antropológica y filosófica, Thomas Hobbes, encuentra en él semejante un enemigo y en el miedo, una relación contundente con la organización política; por cuanto, el estado natural se encuentra fundado en el predominio de la fuerza y el egoísmo como esencia de los seres humanos, lo cual lo lleva a anteponer su propia existencia sobre la de los demás.

De allí que, la vida en esta época primigenia sea brutal y corta, sumado a una guerra desmesurada, en razón de su carácter conflictivo, dado a que sus instintos naturales, acarrean la destrucción de la especie.

Es así como, su única escapatoria para las personas racionales es ceder libertad a un soberano en aras de auto conservarse; tan anhelada cesión justifica su sumisión al orden y con ello derivara en entender el surgimiento del Estado.

Hobbes señala:

> La causa final, fin o designio de los hombres (que naturalmente aman la libertad y el dominio sobre los demás) al introducir esta restricción sobre sí mismos (en la que los vemos vivir formando Estados) es el cuidado de su propia conservación y, por añadidura, el logro de una vida más armónica. (Hobbes, 2019, p.139).

Ergo, una explicación racional del origen de la estatalidad, a través del miedo como fundador de la vida en sociedad, es en el pensamiento hobbesiano, su principal contribución, puesto que pretende acreditar la existencia de una entidad sobrehumana: el Leviatán.

Una figura metafórica para referirse al Estado, ese "Dios mortal" no es otro que el Estado mismo, entendido como pluralidad de voluntades que confluyen en una, cuya finalidad máxima es la seguridad de quienes la conforman, garantizando el bien común para todos.

En este sentido, su poder es absoluto e ilimitado, al ser una expresión del interés general. El único criterio de legitimidad, se enmarca a lo que dicte el Estado, el cual consiste no sólo en prescribir normas, sino también en establecer qué ha de entenderse por juicios morales o de reproche (bueno-malo) teniendo siempre de la finalidad de asegurar el orden y mantenerlo (Camps, 2017).

De esta manera, se prioriza la seguridad y la paz sobre la libertad individual, esta última es un valor que debe ser limitado por el soberano, por ello al desafiar su estructura misma, por rebeldía u otras razones, se considera una amenaza directa al orden social, convirtiéndose en el delito más grave de todos y es desconocer el pacto fundacional de Estado.

Para Hobbes, "todo cuanto el soberano hace en virtud de su poder, se hace por la autoridad de cada súbdito y, por consiguiente, quien realiza una acción contra el soberano, la efectúa, a su vez, contra sí mismo" (Hobbes, 2019, p.182).

En consecuencia, se colige, la imposibilidad de un derecho de rebelión frente al Estado, dado al pacto originario que busca garantizar la seguridad de los individuos; por ello, se genera un proceso excepcional para procesar a las personas que desconocen la autoridad de la soberanía "esto es, no como a malos ciudadanos sino como a enemigos del Estado*"* (Saidiza & Carvajal, 2016, p. 22).

Para el caso en concreto, el súbdito que niega al soberano, rompe el pacto social y pasa a ser considerado enemigo externo, pues ya no está amparado bajo las leyes que regulan a los miembros del pacto.

Con ello, se está ante la presencia de un derecho de guerra, por el peligro que supone el individuo frente a la existencia del pacto social, una clara agresión legítima al Estado a ejercer su fuerza, el cual puede ser castigado incluso eliminado sin restricción legal ya que la negativa del reconocimiento lo deja fuera de la comunidad política.

Es con el ideario liberal de John Locke, donde el Leviatán comienza a fracturarse y se erige un Estado liberal encaminado al reconocimiento y prevalencia de derechos individuales; convirtiéndose en su finalidad primordial.

Para este filósofo, el estado naturaleza difiere en gran medida sobre el de Tomas Hobbes; en primer lugar, el estado primigenio no existe la anarquía ni la guerra, sino deriva del orden de la naturaleza, una pacificidad guiada por la voluntad de Dios, es un estado de apoyo y preservación mutua donde todos los hombres poseen su libertad y producen lo necesario para subsistir.

En segundo lugar, uno de los derechos que se encuentran dentro de este estado naturaleza, es el derecho a la propiedad, connatural a la esencia de conservación de su especie ya que el ser humano tiene la necesidad de apropiarse de los recursos básicos que faculte su subsistencia.

Tal derecho natural consolida el núcleo de la libertad individual, puesto que, la misma se centra en la capacidad de poseer, empezando por su posesión propia y el trabajo que le asiste (Camps, 2017).

Bajo este derecho de propiedad, para Locke la economía antecede históricamente a la constitución del Estado y es precisamente este factor el que lo crea, cada sujeto al apropiarse de recursos, inexorablemente cae en el exceso de acumulación o ambición, pues el surgimiento de la propiedad privada a partir del trabajo va configurando una distribución desigual de recursos que incide en una serie de conflictos que impiden conservar la libertad (Camps, 2017).

De esta forma, surge la necesidad del surgimiento del Estado, para proteger la propiedad privada pero también para limitarla, edificando una tendencia implícita en la humanidad de buscar un orden social al establecer que la libertad individual prevalece; pero queda vedada a los propios fines para los que fue creado (garantizar libertades).

Por tanto, el ejercicio de un poder arbitrario no se puede considerar un poder legítimo, pues vulnera de manera violenta la libertad que lo ha regido; es así como, funda el derecho a la resistencia ya que pone en consideración que, si el contrato tácitamente establecido deja de cumplirse, el pueblo ha de tener derecho a sublevarse y derrocar a quien detenta el poder.

Según los doctrinantes Hugo Fernando Saidiza Peñuela y Jorge Enrique Carvajal Martínez (2016), en su obra establecen que:

> Si este fin no se cumple –el de salvaguardar los derechos naturales- o se presenta un abuso de poder por parte del soberano, los ciudadanos quedan en libertad de derrocarlo y establecer otro gobierno, consagrándose en el pensamiento lockeano el derecho a la rebelión –en contraposición a Hobbes donde no hay lugar a tal derecho (p.23).

Es así como, funda el derecho a la resistencia ya que pone en consideración que, si el contrato tácitamente establecido deja de cumplirse, el pueblo ha de tener derecho a sublevarse y derrocar a quien detenta el poder, cuando el estado mismo va en contra de los postulados en los que se erige.

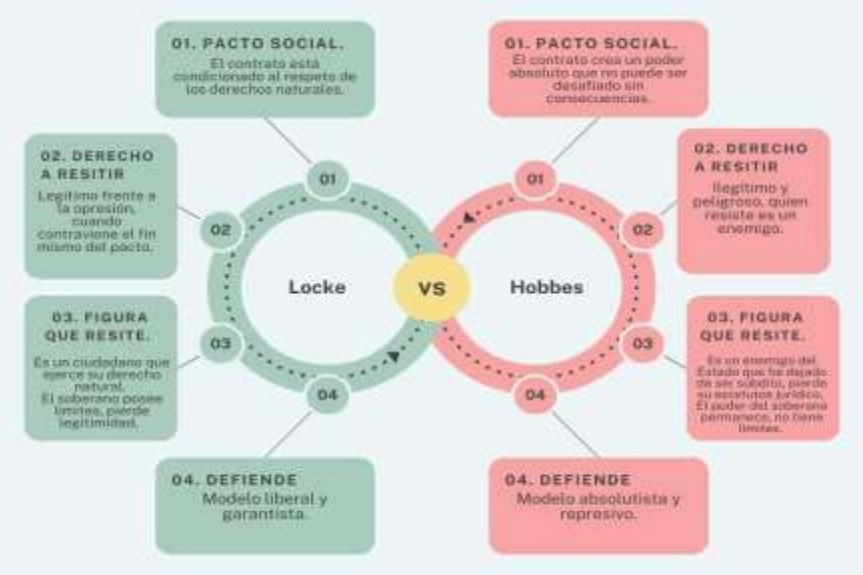
Así las cosas, es con Locke que se comienza a limitar la seguridad pública a partir de los derechos naturales, es decir, no todo vale, si bien el Estado posee un poder inmenso desde una visión liberal queda delimitado a garantizar los derechos.

De allí, que de existir un abuso del poder, las personas pueden ejercer resistencia ante tales actos que menoscaben su dignidad, lo cual, no los deja por fuera del ordenamiento, sino que buscan volver a reconstruir los pilares en los que se cimentó el Estado.

Conviene señalar que Eugenio Zaffaroni (2011) dispone que este derecho de rebelión o resistencia a la opresión es el punto más notorio de diferencia entre ambas teorías contractualistas.

Figura 1.

Comparación del Contractualismo Locke y Hobbes.



Fuente: Elaboración propia tomado de Zaffaroni (2011a).

En síntesis, el contractualismo postula una igualdad y libertad abstracta inherentes al ser humano, las cuales son cedidas mediante un pacto con el fin primordial de salvaguardar derechos fundamentales y garantizar su seguridad.

De esta cesión emerge el Estado, un ente artificial que, una vez constituido, trasciende su origen individual para ejercer legítimamente la fuerza y el derecho en aras de su propia integridad y la protección del orden social.

Con el tiempo, ambas visiones referenciadas han ido evolucionando, en teorías más complejas; no obstante, no se abandona la idea de que el Estado debe brindar a su población un entorno de orden público, convivencia pacífica en comunidad ya sea, priorizando la seguridad, privilegiando la libertad, o proponiendo un equilibrio razonable entre ambas.

En este orden de ideas, la seguridad pública emerge como un fin esencial del Estado, arraigado en el instinto primario de supervivencia del ser humano, lo que históricamente impulsó

el tránsito del estado natural a organización civil. El referido concepto, además de consolidarse como un objetivo estatal fundamental, ha trascendido para convertirse en un derecho fundamental de profunda relevancia para la comunidad.

Bajo esta premisa, es un derecho cuyo contenido siempre ha quedado supeditado a proteger garantías individuales, en otras palabras, como un marco de protección que debe brindar el Estado para permitir el ejercicio libre y efectivo de los derechos de todo el que reside en él.

Su efectividad, recae en las pautas de convivencia que se deban tener por parte de la comunidad y en el monopolio de la fuerza del Estado, al ser una facultad legítima y exclusiva para emplear medios coercitivos en su territorio, a través del sector de defensa y la rama judicial.

Empero, el tercero que adquiera dichas características sin ser autorizado por el Estado implica una amenaza latente contra el ordenamiento, reflejando una crisis de legitimidad.

2.1.2. Terrorismo Tradicional: Un Estudio de sus Formas y Manifestaciones

A partir de este marco, ha existido una difusa línea entre el derecho a resistir y una eventual vulneración a la seguridad pública como derecho fundamental, lo cual, plantea la dificultad de establecer en qué momento ejercer oposición o desafiar la autoridad configuran un accionar legítimo que salvaguarda derechos fundamentales; en contraposición con representar un peligro existencial para la colectividad misma.

La construcción de estas categorías, en la actualidad se encuentran en una lucha permanente.

Generalmente, constituye una tarea dispendiosa a nivel socio jurídico tratar de buscar la diferencia entre un accionar legítimo en uno ilegítimo que configure un riesgo al orden social; para ello se han implementado dos figuras jurídicas que pueden confundirse o utilizarse de manera ambigua conforme a la dialéctica que genere el grupo o el Estado en cuestión.

En ese sentido, el terrorismo y la rebelión, son formas disimiles en naturaleza y objetivos; en primer lugar, la rebelión se dirige a ser una lucha abierta en búsqueda de sustituir el orden político y constitucional, convirtiéndose en materia penal en delitos políticos que se configura de distintos medios desde "la violencia revolucionaria, la lucha armada, la asonada, la insurrección o la sedición como mecanismos para trastocar la institucionalidad y generar formas otras de gobernabilidad"(Mesa C, 2022, p.125).

En ese ámbito, tiene un móvil una intencionalidad política "que anclan sus motivaciones en el "derecho a la resistencia insurreccional" cuando consideran las instituciones y sus gobiernos como agresores, injustos" (Mesa C, 2022, p.125), en aras de modificar la estructura del poder o cambiar la realidad institucional a nivel jurídico, político y social.

Se debe tener en cuenta que la esencia de este trato diferencial en el actuar con finalidad política permite, que cualquier conducta desarrollada en el marco de la rebelión estaría conectada con dicha finalidad, ampliando su alcance.

No obstante cualquier acto que desnaturalice el levantamiento en contra de la autoridad y busque vulnerar a la población; así como transgredir los principios rectores del DIH, se desvela el verdadero trasfondo del fenómeno, revelando su naturaleza como acto terrorista

Por otro lado, se encuentra el terrorismo, agudizando escenarios donde el Estado enfrenta amenazas que trascienden la criminalidad común e implica el abandono del proyecto político, encontrando su asidero en toda actividad "dirigida a desestabilizar la de forma violenta el sistema político-institucional, necesariamente debemos partir de la existencia de un poder estatal legítimo y democrático" (Nieves & Sanz, 2019, p. 309, citado en Mesa, 2022, p. 130).

Existe una violencia sistemática e indiscriminada en este fenómeno, con métodos clandestinos que buscan lograr infundir el miedo, ese impacto psicológico, estratégico que puede tener o no fines políticos y económicos, pero se considera ilegítimo por su desproporción e impacto sobre la población civil, pues su manifestación queda excluida del DIH.

En efecto, bajo esta premisa, dentro de la normatividad existe un tratamiento más indulgente al rebelde que al terrorista; en vista de que como delito político incorpora un carácter altruista, impulsado por un interés colectivo de mejorar a un estado injusto relegando intenciones egoístas y dañinas para la colectividad.

Según Sentencia C-009 de 1995 de la Corte Constitucional cuyo Magistrado Ponente es Vladimiro Naranjo Mesa dispone:

> Si bien es cierto el fin no justifica los medios, no puede darse el mismo trato a quienes actúan movidos por el bien común, así escojan unos mecanismos errados o desproporcionados y a quienes promueven el desorden con fines intrínsecamente perversos y egoístas. Debe, pues, hacerse una distinción legal con fundamento en el acto de justicia, que otorga a cada cual lo que merece, según su acto y su intención (Corte Constitucional, 1995a, Sentencia C-009 de 1995).

Con esto en mente, mientras algunos movimientos buscan reivindicaciones políticas mediante el uso de la fuerza, otros recurren a la violencia indiscriminada ya sea en beneficio propio o de un tercero, a partir de infundir terror y desestabilizar el orden social; de allí que se observe un carácter subjetivo del agente, es decir si su intención se encuentra originada por una finalidad de cambiar el statu quo.

Resulta pertinente resaltar, que existe un sin número de definiciones del concepto del terrorismo, teóricos holandeses como Alex Schmid y Albert Jongman de la Universidad de Leiden, generaron una recopilación de definiciones académicas oficiales sobre el fenómeno, llegando a un consenso sobre los elementos reiterativos que lo componen:

Figura 2.

Elementos del Terrorismo.

Fuente: Elaboración propia con base en Schmid, A. P., & Jongman, A. J. (1988), citado por Chaliand, G., & Blin, A.. (2017).

Ahora, si bien son parámetros útiles a la hora de conocer qué elementos son reiterativos en el terrorismo, visibiliza la ambigüedad para rastrear un consenso académico que demarque su esencia, o que lo diferencie de otras formas de violencia, complicando su tratamiento teórico, jurídico y político al momento de diferenciarlo frente al derecho a resistir.

Su variabilidad conceptual, dota al término de un carácter dinámico en la historia, adaptable a diversas narrativas y contextos políticos, ideológicos, jurídicos de cada época por actores estatales y no estatales quienes pueden emplearlo para legitimar o deslegitimar diferentes actos de violencia; moldeando conflictos sociales a gran escala.

A partir de lo señalado, esta situación llevó a delimitar los teóricos incluidos en este trabajo, centrados en la construcción histórica del terrorismo; en ese sentido, se destacan las contribuciones de tres expertos en la materia: David Rapoport, Gérard Chaliand y Arnaud Blin, así como Andrade Becerra, cuyas obras ofrecen un análisis histórico y genealógico del concepto, cuyo pensamiento puede agruparse de la siguiente manera:

Tabla 2.

Evolución del Terrorismo.

Evolución del Terrorismo.	
Terrorismo Antiguo.	Sus antecedentes se encuentran en sectas de medio oriente y asiáticas que empleaban la violencia selectiva para desestabilizar regímenes, con ciertas características en común: ● Sectas conformadas por minorías étnicas o religiosas pero organizadas y efectivas. ● Modus operandi dirigido al asesinato de personas publicas pertenecientes al gobierno, desarrollo de la figura del tiranicidio eliminación violenta de un tirano cuando este actuaba en contra del bien común. ● Fines religiosos y simbólicos: defender sus creencias, autonomía frente a otros grupos. Utilización de armas artesanales, tendiente a convertir los asesinatos en actos sacramentales y legítimos de origen mesiánico.
Terrorismo Edad Media.	El uso del terrorismo en las guerras religiosas es simplemente un fenómeno secundario, se resalta la Guerra de los Treinta años 1618 a 1648 y los acuerdos firmados en Westfalia en 1648 que p fin a las luchas por religión y a las campañas de terror que los acompañó.
Terrorismo Moderno.	**Revolución Francesa (1789)**
	Primer antecedente, punto de inflexión el término "terrorismo" o lo que podría llamarse "terrorismo de Estado" fue utilizado por primera vez durante la Revolución Francesa, esto frente a los jacobinos error revolucionario francés que azotó los años 1793 y 1794. al utilizar el terror como un instrumento de control político, concepto del enemigo interno frente a los rebeldes y naciones extranjeras.
	Oleadas del Terrorismo.
	Ola Anarquista 1880-1920.
	En Europa guiado por ideales libertarios, anarquistas, nihilistas, surgió un nuevo tipo de terrorismo no religioso, practicado por grupos marginales influenciados por el romanticismo en aras de derrocar gobiernos despóticos o tradicionalmente concebidos, atentados, que involucros atentados contra figuras de autoridad; en conjunto, con el protagonismo de la prensa, con el uso de la "propaganda por acción" comenzó a adquirir dimensiones internacionales. Geopolíticamente, el siglo XIX vio el declive del orden de Westfalia, el auge del nacionalismo y la inestabilidad en regiones.
	Ola Anticolonial 1920-1960.
	Tras la I Guerra Mundial, que dio como resultado el Tratado de Versalles el cual reconoció el principio de autodeterminación, libro a la organización a desmantelar el producto del colonialismo, en consecuencia, se dirige a la concepción de la lucha por la autodeterminación de los pueblos, en

	procesos descolonizadores y revolucionarios. Todo acto de terrorismo buscaba la liberación de aquellos países oprimidos por la colonialidad.
	Ola de la Nueva Izquierda. 1960-1980.
	Este periodo coincidió el debilitamiento de los grandes imperios, lo que provocó una crisis del orden político internacional y alimentó el auge de nacionalismos e ideologías radicales, en esta etapa los actos terroristas fueron principalmente regicidios cometidos por grupos de extrema izquierda, producto de ideologías marxistas, imperialistas y leninistas. De igual manera, conto con la implementación de regímenes totalitarios de corte europeo (Alemania, Unión Soviética, España, Italia) el terrorismo se asoció no solo a movimientos sino también estos Estados encontraron en el terror una herramienta intrínseca del poder, inicio y fin de la II Guerra Mundial.
	Ola Religiosa. 1979- Presente.
	Le antecede la Guerra fría, se utilizaron por parte de los Estados a movimientos inconformes para la realización de actos terroristas en otros Estados con el objetivo de desestabilizarlos en la lucha contra el bloque capitalista y comunista. La oleada, nace de la Revolución Iraní 1979, hubo el surgimiento del terrorismo islámico a nombre de la yihad, justificación de la violencia en la doctrina religiosa musulmana, herramientas como las bombas, fundación de Al-Qaeda, ven en Occidente un enemigo dado su se dirige contra amplios sectores civiles, incluso sin conexión directa con el conflicto en aras de restaurar el orden religioso. Karl Heinzen, padre del terrorismo moderno, propuso la ampliación del concepto de tiranicidio, legitimando el asesinato masivo como instrumento necesario, bajo la idea de que la violencia podía ser moralmente válida si se dirigía al derrocamiento de sistemas opresores.
Terrorismo Contemporáneo.	**Terrorismo Internacional.**
	Para la historia del terrorismo contemporáneo, existen cuatros puntos de inflexión de gran relevancia para desarrollar lo que en la actualidad se refiere a terrorismo internacional, caracterizado por su enfoque transfronterizo involucrando distintitos actores, victimas y estados a menudo con base religiosas o políticas: ● 1968. Desarrollo de las guerrillas urbanas latinoamericanas y la estrategia de los palestinos iniciaran la tacita del terrorismo como propaganda que escaló a violencia. ● 1979. Revolución Iraní impulsando el chiismo radical y el martirio, e intervención soviética en Afganistán aprovechada por EEUU para apoyar a islamistas sunitas radicales contra la URSS, en contexto de Guerra Fría. ● 1983. Cuartel de los Marines en Beirut, que ilustró la letalidad del terrorismo suicida y la creciente implicación de actores no estatales en conflicto.

	● 2001. A partir de la ola religiosa, intervención en países musulmanes, genero cambios de política de seguridad en especial en Estados Unidos y con ello el ataque histórico el 11S que tajo consigo la aparición del terrorismo global, catalizó la "Guerra contra el Terror" y evidenció la capacidad de organizaciones transnacionales para llevar a cabo ataques de gran escala con consecuencias geopolíticas profundas.
	Ciberterrorismo: Terrorismo Informático o Digital.
	Con la implementación de la tecnología auspiciado por la interconexión global que proporciona el internet, el terrorismo ha adquirido una desarrollo más flexible y descentralizado, cuya propaganda y ataque se realiza a través del espacio cibernético, dando paso a nuevas formas de amenaza, actores y métodos.

Fuente: Esquema propio con base en una síntesis de la evolución del terrorismo realizadas por Andrade(2014 p. 3-10), Rapoport (2004) y Chaliand & Blin (2017).

En efecto, se colige que la figura del terrorismo es un fenómeno diverso, que se delimita conforme a cada caso en concreto, si bien, la sociedad, es una institución viviente compleja, por su naturaleza ha conducido reiteradamente a situaciones de conflicto por diversos factores como lo económico, político, religioso, cultural etc.

De allí, que cada conflicto comprende una esfera propia de particularidades específicas que lo diferencien de otro, por lo que implica variación y percepción de la figura del terrorismo.

En principio, la historia del fenómeno se remonta a ir en contra de los postulados de un orden local, convirtiéndose en grupos jerarquizados y organizados en el desarrollo de sus actividades que con el tiempo comenzaron a trascender fronteras territoriales y a ser un problema para la comunidad internacional.

Lo anterior, debido a los ataques del 11 de septiembre de 2001 en el territorio estadounidense por el grupo terrorista Al Qaeda, que se convirtieron un punto de inflexión en la seguridad internacional, al observar como una gran potencia podía ser objeto de actos de violencia sin precedentes.

Es así como, el terrorismo encontró en estos ataques, el impulso que requería para observar cómo diferentes organizaciones podrían operar a escala global desafiando la seguridad no solo de

un país, sino de varios de ellos, infligiendo de manera brutal, el mayor daño posible a la población logrando miedo e incertidumbre en todo el mundo.

Con ese propósito, Estados Unidos y sus partidarios, comenzaron a generar acciones en aras de desmantelar redes terroristas, estrategia denominada "guerra contra el terrorismo", cuyo participe activo fue la Organización de Naciones Unidas (ONU).

Como se ha mencionado, a lo largo del tiempo, diversas conceptualizaciones han sido formuladas, sin embargo, es a partir de este acontecimiento que Estados Unidos consolidó una definición con gran impacto internacional.

Desde un punto de vista práctico, el Departamento de Estado de los Estados Unidos citado en el estudio de Chaliand & Blin (2017) realiza la siguiente definición: "el terrorismo es premeditado, violento con motivaciones políticas perpetrada contra objetivos no combatientes por grupos agentes estatales subnacionales o clandestinos, generalmente diseñados para influir en la audiencia"(p.13)

Vista la información aportada y considerando lo expresado por la Asamblea General aprobada en 1994 la Resolución 49/60 denominada Medidas para eliminar el terrorismo internacional, en cuyo párrafo 3 señaló que el terrorismo parte de:

> (...)actos criminales con fines políticos concebidos o planeados para provocar un estado de terror en la población en general, en un grupo de personas o en personas determinadas» y que esos actos son «injustificables en todas las circunstancias, cualesquiera sean las consideraciones políticas, filosóficas, ideológicas, raciales, étnicas, religiosas o de cualquier otra índole que se hagan valer para justificarlos (p.1).

Con esta última claridad conceptual, adaptada al contexto de la época, el terrorismo en la actualidad connota una violencia insurgente y no estatal, pero este no debe ser confundido con los movimientos guerrilleros.

A pesar de que son actores no estatales que participan activamente en conflictos armados de carácter no internacional, presentan unas características especiales al ser actores políticos, desarrolladas por los Tratados de Ginebra, en particular el Protocolo II que se dirige a regula los conflictos internos de los Estados (Naciones Unidas, 1977b).

Con esto en mente, para comprender la esencia del fenómeno se debe analizar sus elementos esenciales que lo diferencian de otros y delimitan su marco a operar estos son:

Figura 3.

Elementos conceptuales del Terrorismo.

Fuente: Esquema propio con base en párrafo 3. Resolución 49/60 de 1994.

- Actor No Estatal: El Estado bajo el pacto social está legitimado para ejercer el monopolio de la fuerza; en consecuencia, el terrorismo se asocia primordialmente con la violencia perpetrada por grupos, organizaciones o individuos que operan al margen de la autoridad estatal legítima.
- Objetivo Ideológico: Cada grupo generalmente está estimulado por diferentes objetivos de origen político, cultural, religioso, económico, etc. De allí, su naturaleza multifacética; se erige como medio adaptable y flexible para fines diversos.

- Violencia física o amenaza: Elemento objetivo, materialización de un acto simbólico estratégico y premeditado que busca generar una presión a favor de las demandas de quienes la realizan, causando daño físico o psicológico a personas por distintos métodos. De igual manera, la amenaza del acontecimiento es igual de poderosa que la materialización de la conducta; la difusión de un posible evento físico, crea un clima de inseguridad e imprevisibilidad.
- Daño a la Población Civil: Es el resultado con esta práctica, la población no combatiente se convierte en instrumentos selectivos, los ataques se dirigen a lugares públicos con gran afluencia. El resultado es la pérdida de vidas inocentes, lesiones físicas y traumas psicológicos profundos en individuos que, en muchos casos, no tienen una conexión directa con el conflicto o la causa que alegan defender los terroristas.
- Producción de miedo, terror o zozobra: Elemento subjetivo, el terrorismo es una estrategia basada en el impacto psicológico, se busca crear o inducir a la comunidad a un estado de perturbación emocional, ampliando el rango; es decir, no solo a la víctima directa sino al colectivo, logrando permear la vida cotidiana, alterando la tranquilidad pública y estableciendo una conexión con la amenaza e ideológica subyacente.
- Inobservancia del DIH: Sus métodos y objetivos a menudo implican la violación sistemática de los principios fundamentales del DIH, especialmente la protección de la población civil.

En conclusión, los elementos previstos convergen para dar cuerpo al fenómeno del terrorismo, al interactuar dinámicamente, configuran una forma de violencia singularmente diseñada para subvertir el orden, influir en la política y sembrar el terror en sociedades enteras, representando un desafío constante a la seguridad, la estabilidad y los principios humanitarios a nivel global.

Hecha esta salvedad, y una vez comprendido el impacto global, se observa como cada instrumento adoptado por la lucha contra el terrorismo se condensa en el área en la justicia penal, según la Oficina De Las Naciones Unidas Contra La Droga Y El Delito (2018);

> En la mayoría de los instrumentos universales se adopta un enfoque de la lucha contra el terrorismo con base decididamente en la justicia penal. Esto significa que los sistemas judiciales penales y las instituciones policiales nacionales son los principales impulsores del sistema. La actuación coordinada de las autoridades policiales, los fiscales y los jueces es un elemento fundamental de este enfoque (p.51).

Con esto en mente, en un ámbito de compromisos y obligaciones, los Estados con arreglo al derecho internacional, se centraron en condenar de manera ineludible toda actuación terrorista a través de un ordenamiento de persecución y sanción como lo es el Derecho Penal, como respuesta efectiva ante conductas que pongan en peligro la estabilidad pública y la seguridad de las personas.

A tal efecto, los Estados miembros adoptaron un enfoque legislativo punitivo robusto para enfrentar el terrorismo, integrando las disposiciones internacionales y regionales que permitan una respuesta ante esta amenaza global.

Lo cual, implica no solo la creación de normas penales específicas que tipifiquen las conductas terroristas, sino también una cooperación internacional activa que permita una lucha integral y coordinada contra el terrorismo en todas sus formas.

2.1.3. Nuevo Terrorismo: Ciberterrorismo.

En la actualidad, la tecnología ha cambiado la forma en cómo el ser humano percibe el mundo; ya que, el hombre impulsado por su necesidad de relacionarse en comunidad género herramientas comunicativas que trascienden sus propios alcances.

Entre ellas, destacan las redes de telecomunicaciones a nivel global, que constituye una compleja red de interconexiones de distinta naturaleza, donde se almacena una infinidad de datos de carácter informático, al permitir la continua comunicación entre personas, instituciones y

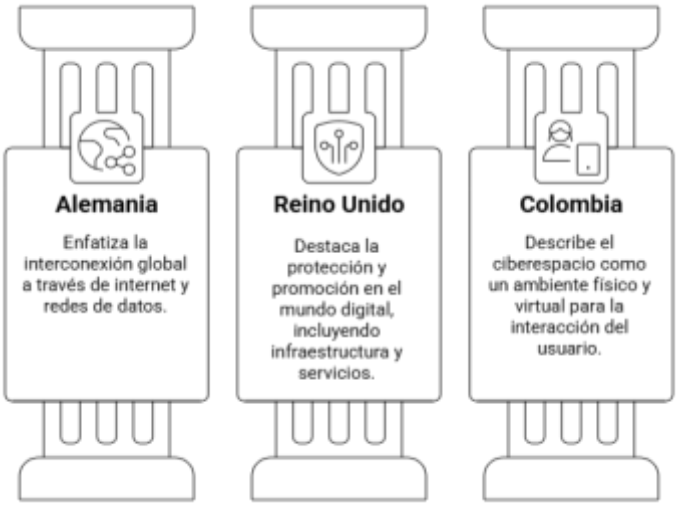
sistemas automáticos. No obstante, más allá de la mera utilidad funcional, quienes utilizan las telecomunicaciones han generado un nuevo ámbito social y político: el Ciberespacio.

En el Ciberespacio convergen múltiples redes de telecomunicaciones, que permiten la transmisión de datos en tiempo real, facilitando desde la interacción interpersonal hasta el funcionamiento de complejos sistemas automatizados; sin embargo su conceptualización o delimitación es compleja por cuanto su definición continúa en construcción, al ser un fenómeno relativamente reciente y paradójicamente complejo.

Entre las conceptualizaciones generadas se tiene las presentadas por diferentes departamentos de ciberseguridad del mundo que son analizados por Steven Jones Chaljub (2022) en su obra denominada “Conceptualización del Ciberespacio humano”, para efectos del presente trabajo, se tomarán en consideración tres de estas definiciones en particular, por su relevancia y utilidad en el abordaje del tema.

Figura 4.

Conceptualización Global del Ciberespacio.



Fuente Elaboración propia en Nankín con base en Jones-Chaljub, S. (2022).

Bajo estas premisas, el Ciberespacio no solo incluye la dimensión física (dispositivos, cables, servidores, routers), sino también la dimensión virtual (datos, programa, protocolos y contenidos generados por los usuarios); no obstante, es el segundo componente el más peligroso.

Lo anterior, por cuanto el componente físico es el medio por el cual el entorno virtual se materializa y este último gestiona flujos masivos de información que conforman comportamientos y opiniones, al interactuar con distintas herramientas de comunicación tecnológica lo que genera determinados problemas sobre manipulación, vigilancia y control.

El Ciberespacio es una zona sociotécnica, que permea todas las instancias de la vida social, emergiendo como la infraestructura para el tratamiento de datos informáticos por excelencia que en la actualidad es un pilar para la economía y la sociedad.

De hecho, diversos autores como Mayer Schonberger, Kenneth Cukier (2013) e incluso Manuel Castells (2009) denominan este momento histórico como la "era del dato" o "la era del big data"; un periodo marcado por la producción, recolección, tratamiento y circulación masiva de información personal, institucional y/o gubernamental, un fenómeno comparable a la Revolución Industrial.

En esta nueva forma, los datos se convierten en un bien estratégico, capaz no sólo de generar valor económico, sino de adaptar o moldear comportamientos sociales, influir en decisiones políticas y/o transformar relaciones de poder contemporáneo, al poseer, un componente virtual-en especial el internet y las redes sociales- el Ciberespacio se edifica como una herramienta sofisticada de control social.

A razón de lo anterior, la figura se convirtió en un nuevo dispositivo de control social informal en la era contemporánea, el cual llega a ser una variante controladora, que genera una pérdida de intimidad del individuo, quien gustoso cede y legítima su desarrollo.

Bajo este referente, el liberal y ciberactivista John Perry Barlow, en su manifiesto de 1996 denominado "Declaración de independencia del Ciberespacio", refiere a un mundo virtual,

soberano autogobernable, sin intervención de las autoridades estatales ni su normatividad, el autor expone:

> Nuestro mundo es diferente. El Ciberespacio está formado por transacciones, relaciones y pensamiento en sí mismo, que se extiende como una quieta ola en la telaraña de nuestras comunicaciones. Nuestro mundo está a la vez en todas partes y en ninguna parte, pero no está donde viven los cuerpos (Barrow, 1996, p.2).

Para el autor, los conceptos legales no entran en esta órbita dado a que estos están con base s en la materia y este mundo no está con base en ella.

Asimismo Johnson y Post (1996), destacados juristas, en el mismo año, en su artículo "Derecho y Fronteras: El Auge del Derecho en el Ciberespacio" continúan con el planteamiento de Perry, ante la imposibilidad de los estados de la regular el entorno digital globalizado y transfronterizo, que escapa de su jurisdicción y establecen que la única alternativa es la autorregulación de quienes intervienen en él.

No obstante, a pesar de los planteamientos comentados, el Estado en conjunto con las organizaciones internacionales tomaron la iniciativa y comenzaron a regular algunas áreas de esta categoría tan extensas; a petición precisamente de los particulares que eran víctimas de hurto de datos masivos, virus informáticos, estafas y daño en sus sistemas.

La vulnerabilidad de los sistemas informáticos originó que el Ciberespacio se transformara en un nuevo frente de crimen organizado, con conductas que posteriormente fueron consideradas como punibles en el ámbito global configurando la categoría de ciberdelitos.

Los ciberdelitos o delitos informáticos, son complejos de conceptualizar por la novedad de las conductas, para el criminólogo Majid Yar (2006) citado por Gustavo Sain 2018, "la delincuencia informática se refiere no tanto a un único distintivo tipo de actividad delictiva, sino más bien a una amplia gama de actividades ilegales e ilícitas que comparten en común el único medio electrónico (Ciberespacio) en el que tiene lugar "(p.9)

El anonimato y la extraterritorialidad de los ciberdelitos, originaron una genuina preocupación de la comunidad internacional por la prevención, resistencia y recuperación de infraestructuras informáticas, lo que obligó al desarrollo de un andamiaje legal punitivo para contrarrestar la amenaza.

De esta manera, desde los años 80 han existido una serie de documentos por organizaciones internacionales buscando la persecución de estas conductas; no obstante es la OCDE (Organización de Cooperación y Desarrollo Económico) que comienza a sembrar el camino en 1982 al convocar a una serie de expertos para ajustar la legislación penal a las necesidades informáticas.

En 1989, le sigue el Consejo de Europa, con una serie de directrices a sus países miembros para abogar por estos delitos, a su turno la ONU en el Octavo Congreso sobre la Prevención del Delito y Tratamiento del Delincuentes lo consolidó como un tema de su agenda internacional.

No obstante, no fue hasta 2001, que fue concebido el Convenio de Budapest sobre la ciberdelincuencia, primer tratado internacional promovido por el Consejo de Europa que pretende la adopción de tipos penales de carácter informático.

Según Gustavo Sain (2018) el referido convenio establece una serie de tipologías concernientes al *"*ámbito de la cibercriminalidad como modelo legislativo, tanto en el ámbito de Derecho Penal como procesal penal; principios generales de cooperación entre los diferentes países en materia judicial y procedimientos vinculados a la investigación criminal" (p.14)"

El tratado de Budapest influyó en gran parte en la legislación penal Colombiana, si bien en su momento no fue signatario del convenio, sus lineamientos en conjunto con los informes de la OCDE, las alianzas con la ONU y la OEA, influyeron en la redacción de la Ley 1273 de 2009 "Delitos contra la información y los datos".

Lo anterior, condujo a la formulación de nuevos tipos penales informáticos, como resultado directo de la creciente preocupación por la seguridad digital a nivel nacional e internacional, frente

al incremento sostenido y la complejidad de los ciberataques, así como la presión de organismos internacionales.

El marco jurídico abordado, trata de distintas conductas punibles como: el acceso ilegítimo a los sistemas informáticos, la interferencia ilegítima de la red, la interceptación a los datos informáticos, el daño a la información informática y la vulneración de datos de carácter personal, entre otras.

Su propósito, fue la protección de bienes jurídicos como: la seguridad, la integridad y la confidencialidad de la información en el Ciberespacio, elementos cruciales para el desarrollo de una sociedad digital confiable y segura **(**Piñón et al., 2023).

Cabe destacar, que la Corte Constitucional desde la afamada Sentencia T-414 de 1992 del (1992c, M.P. Ciro Angarita Barón) y las que le siguen (Sentencia SU-082 de 1995, M.P. Jose Arango Mejía; T-729 de 2002, M.P. Eduardo Montealegre Lynett) desarrollo el artículo 15- consagra el derecho a la intimidad y habeas data- limitando a particulares o entes estatales frente abusos del poder informático en el tratamiento de datos personales.

A su vez, consagra la figura de la libertad informática como "una nueva dimensión social de la libertad individual diversa y por razón de las circunstancias que explican su aparición, de otras clásicas manifestaciones de la libertad" (Corte Constitucional, 1992c. M.P. Dr. Ciro Angarita Baron)

Bajo este referente, el ordenamiento colombiano reconoce el dato personal como una extensión de la dignidad humana y no como objeto económico o administrativo; este cambio permitió entender que la vulneración de la información privada en el entorno digital podía constituir una violación directa a los derechos fundamentales, por lo que surgió la necesidad de fortalecer la protección jurídica frente a los riesgos que derivan de ella.

Este desarrollo constitucional, fue otra de las bases para la creación de la Ley 1273 de 2009, que incorporó al Código Penal los delitos informáticos o ciberdelitos, consolidando también la protección penal de la información y los datos personales en Colombia.

Con posterioridad, en 2018, el Congreso de la República aprobó mediante la ley 1928 de 2018 el Convenio de Budapest, cuyo control previo estuvo a cargo de esta misma corte, la cual en Sentencia C-224 de 2019 (M.P Cristina Pardo Schlesinger) declaro la constitucionalidad del apartado reconociendo que:

1. El ciberdelito tiene una naturaleza trasnacional lo que exige mecanismo de cooperación internacional, sin que ello implique pérdida de soberanía.
2. Subrayo que las medidas de investigación que el convenio desarrolla deben ser abordados desde los derechos fundamentales.
3. Su aplicación llega a complementar e interpretar la Ley 1273 de 2009 ya que no permite la protección de sanciones ajenas a las ya previstas.
4. Fortalecimiento de la evidencia digital entre países, como elemento clave para la persecución efectiva de los ciberdelitos.

Con este marco, en materia de jurisprudencial, Colombia comenzó a desarrollar una línea interpretativa de la categoría de los ciberdelitos armonizada con los estándares internacionales y constitucionales.

Labor liderada por la Corte Suprema de Justicia, que se reflejó en Sentencia SP2699-2022 (M.P. Fernando León Bolaños Palacios), la cual, citando los principios y fundamentos del Convenio de Budapest, precisó que la restauración posterior de los datos no excluye la configuración del delito de daño informático, pues lo relevante es la afectación de la disponibilidad y seguridad de la información.

De lo anterior, se concluye, que marco normativo colombiano en torno a los ciberdelitos supone una evolución progresiva, aunque no exenta de lentitud y gradualidad; pues solamente en el plazo de diez años ha mostrado un importante avance.

Este desarrollo expresa un intento de reconciliar la norma nacional con los baremos internacionales y hacer frente a los nuevos desafíos que plantea la criminalidad informática.

A nivel internacional, el Tribunal Europeo de Derechos Humanos, en el caso Buturugă vs. Rumanía (2020)**,** amplió la interpretación del artículo 8 del Convenio Europeo de Derechos Humanos, para incluir la violencia digital y el uso malintencionado de tecnología como forma de vulneración de derechos humanos.

El caso, se dirigió a establecer la inacción que tuvo el Estado rumano al proteger a una mujer víctima que denuncio a su expareja por haber difundido datos de información intima, sin que sobre él se atendiera de manera oportuna y eficaz.

Bajo las jurisprudencias desarrolladas, se observa como el mal uso de la tecnología puede llegar a suponer grandes vulneraciones a los derechos humanos, lo que ha impulsado una reflexión de carácter mundial para la protección del entorno digital.

A pesar de que se han suscitado una serie de avances en protección jurídica frente al Ciberespacio, también ha saltado a la vista nuevos retos vinculados a las transformaciones tecnológicas y a la necesidad de reforzar un gran componente de la seguridad pública actualmente: la seguridad digital.

Según, Tapia Hernández, Ruíz Canizales y Vega Páez (2021)

> (…)o es ajeno el impacto que tiene la globalización en la esfera de los usuarios de internet, cuya preocupación reciente se ha centrado en la denominada ciberseguridad o seguridad cibernética, derivado de los problemas de seguridad, protección de datos y privacidad (p.153).

De igual manera, Resolución A/HRC/20/L.13, de la Asamblea General de la ONU (2012) denominada "*Promoción, protección y disfrute de los derechos humanos en Internet"* afirma que:

> los derechos de las personas también deben estar protegidos en Internet, en particular la libertad de expresión, que es aplicable sin consideración de fronteras y por cualquier procedimiento que se elija, de conformidad con el artículo 19 de la Declaración Universal de Derechos Humanos y del Pacto Internacional de Derechos Civiles y Político (p.2).

Es en este marco de aceleración del término donde el componente virtual del Ciberespacio- dibujado por redes sociales, aplicaciones, plataformas y flujos permanentes de datos- se consolida como un entorno de interacción y desarrollo, pero también como un espacio de alto riesgo. En respuesta, la seguridad digital se contrapone para garantizar la dignidad de los individuos en el desarrollo de su vida virtual.

La seguridad digital se erige como un componente esencial en una sociedad interconectada por las Tecnologías de la Información a nivel global. Su finalidad obra en la preservación del orden y estabilidad social en el Ciberespacio mediante el accionar de los Estados, protegiendo los dominios digitales de sus conciudadanos, al ser una extensión de la intimidad del individuo en la que ejercen derechos fundamentales.

Tabla 3.

Derechos conexos a la Seguridad Digital.

Derechos Fundamentales	**Conexión con Seguridad Digital**
Derecho a la privacidad y Protección de Datos (Habeas Data).	Salvaguarda de datos personales, impide el acceso y utilización de datos de carácter personal sin consentimiento y la protección frente a la vigilancia virtual masiva.
Libertad de Expresión e Información.	El principal medio de comunicación que existe hoy en día es el Internet, por lo que la libertad de opinión, difusión y acceso a la información se ha trasladado a la red.
Derecho a la propiedad (Bienes digitales)	Los espacios virtuales y dominios son una extensión del ámbito del individuo y a su vez activos que deben ser protegidos.
Seguridad Personal y Dignidad Humana.	Protección de datos personales, identidades virtuales, patrimonio electrónico y relaciones familiares en el entorno virtual; ya no abarca solo la protección física de la persona, sino que incluye todas sus dimensiones.

Fuente: Elaboración propia.

Sobre los derechos en un contexto contemporáneo, como la intimidad, habeas data o libertad de expresión, es claro que enfrentan tensiones derivadas del tratamiento de información personal y de grandes volúmenes de datos no consentidos en el entorno digital, que con ciertas lógicas algorítmicas acaparan datos sensibles sin ofrecer mecanismos de control o rectificación; y condicionan el debate público al amplificar o restringir contenidos según intereses particulares.

Por ello, la seguridad digital o ciberseguridad, ha sido identificada como "el conjunto de acciones implementadas para proteger la información presente en el Ciberespacio o en sistemas informáticos interconectados, así como la infraestructura que respalda dicha información"(Piñón et al., 2023, p. 44), convirtiendo en una de las principales preocupaciones de los Estados en pleno siglo XXI, pues trasciende lo técnico para convertirse en un escenario socio jurídico.

A nivel internacional, Europa se ha posicionado como pionera en materia de seguridad digital, entendiéndola desde el componente esencial de protección de derechos como la privacidad, la libertad, dignidad, entre otros. Esta visión ha sido materializada por diferentes fallos del Tribunal Europeo de Derechos Humanos y Tribunal de Justicia de la Unión Europea como:

Tabla 4.

Fallos Representativos de los Tribunales Europeos.

Característica	K.U. vs. Finlandia (2008)	Digital Rights Ireland (2014)	Big Brother Watch vs. Reino Unido (2021)	Schrems II (2020)	Buturugă vs. Rumanía (2020)
Tribunal	TEDH	TJUE	TEDH	TJUE	TEDH
Tema	Responsabilidad estatal por vulneraciones digitales	Retención de datos	Vigilancia masiva	Transferencia internacional de datos	Violencia digital
Decisión	Obligación positiva de proteger la privacidad	Directiva sobre retención de datos inválida	Vigilancia masiva ilegal	Privacy Shield inválido	Violencia digital es violación de derechos
Principios clave	Responsabilidad estatal	Proporcionalidad, limitación	Legalidad, necesidad, proporcionalidad	Seguridad digital transfronteriza	Prevención, investigación, sanción

Fuente: Elaboración propia.

Los pronunciamientos del tribunal europeo demuestran una alto grado en el desarrollo de seguridad digital, al fortalecer los principios más relevantes como la responsabilidad del Estado en relación con las vulnerabilidades tecnológicas, la prohibición de la vigilancia masiva sin control por parte del poder judicial y la posibilidad de hacer un uso ético, proporcionado y transparente de la tecnología.

Por su parte, la Organización de los Estado Americanos (OEA) ha proporcionado un andamiaje jurídico de gran relevancia, uno de sus primeros documentos internacionales fue al Estrategia Interamericana Integral de Seguridad Cibernética (2004) y la Declaración sobre Seguridad en las Américas (2003), reconociendo la seguridad como un componente esencial y obligatorio a regular por los Estados miembros.

Ahora bien, frente al sistema interamericano como la Comisión Interamericana de Derechos Humanos (CIDH) y su Relatoría Especial para la Libertad de Expresión (RELE) han sostenido que la ciberseguridad debe generar un espacio que garantice libertades y la dignidad humana.

En informe de la CIDH (2018) denominado "*Derechos humanos y seguridad digital: una pareja perfecta "*la comisión insiste en basar la seguridad digital en tres principios centrales: necesidad, proporcionalidad y legalidad, evitando prácticas de vigilancia masiva.

En el caso colombiano, este proceso se ha venido desarrollando con cierto retraso-Colombia, comenzó su implementación de manera tardía a partir de los lineamientos en materia política del CONPES 3701 de 2011, la cual va dirigida a la "*Ciberseguridad y Ciberdefensa*".

El Consejo Nacional de Política Económica y Social (CONPES), en el territorio colombiano es el organismo principal de asesoramiento del gobierno en materia de planeación económica y social, su función se dirige a formular, recomendar y articular políticas públicas para el desarrollo socioeconómico del país a partir de la elaboración de documentos puestos a estudios y posterior aprobación en sesión.

El CONPES 3701 de 2011, en el ejercicio de su función orientadora, se origina con el objetivo de fomentar y robustecer la capacidad del Estado colombiano en torno a las crecientes amenazas digitales.

Dicha documentación parte de la constatación de una progresiva dependencia del ser humano respecto a la tecnología y de la sostenida aparición de delitos informáticos, lo que requería una respuesta integral, articulada y coherente de la institucionalidad.

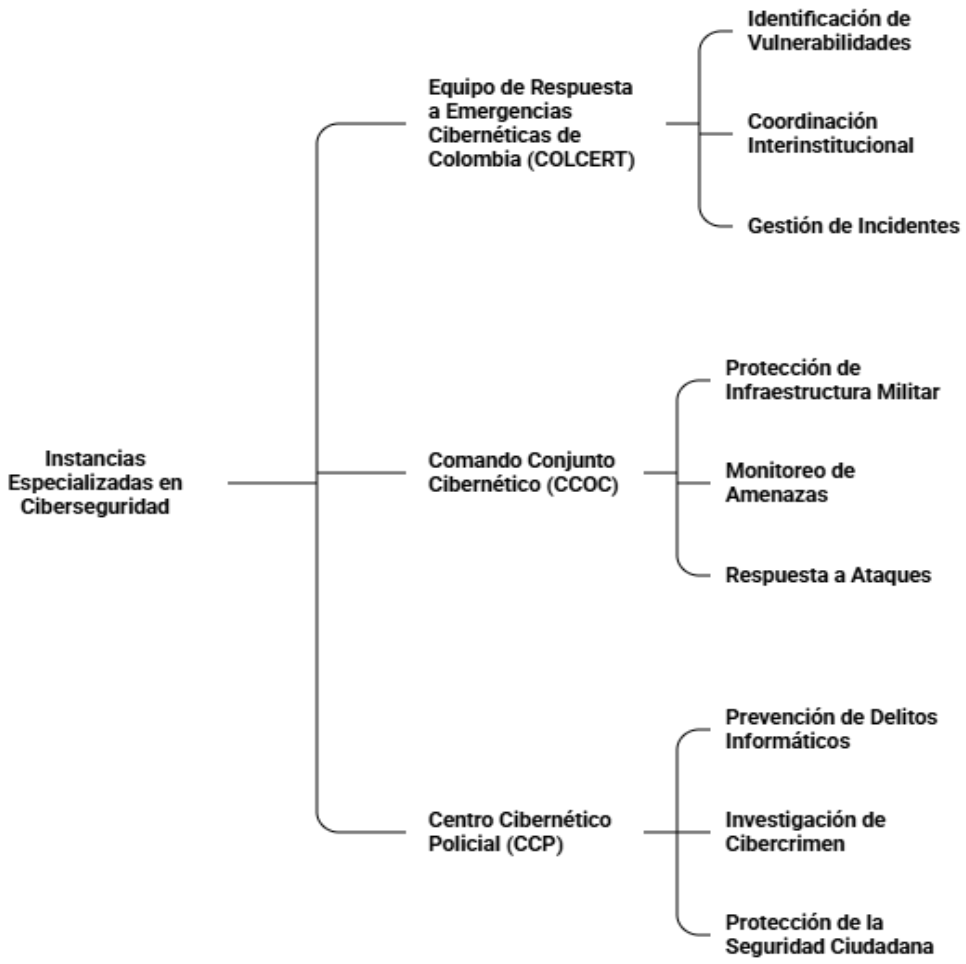
Esta propuesta, constituyó el primer paso para la construcción de una política nacional en ciberseguridad; su esquema se apoyó en tres problemáticas medidas: en primer lugar, la falta de coordinación institucional entre los sectores público, privado y la sociedad civil; en segundo lugar, la escasez de personal especializado en ciberseguridad, lo que limitaba la respuesta ante los incidentes; por último, la insuficiencia en el marco normativo, que no había previsto las nuevas modalidades de delitos informáticos (Consejo Nacional de Política Económica y Social, 2011).

En coherencia con lo mencionado, el CONPES 3701, incorporó la figura del Ciberespacio y con ello invitó a la creación de instancias específicas como COLCERT, CCP y CCOC (la Policía Nacional y las Fuerzas Militares) y las instituciones civiles.

En atención de lineamientos técnicos y estratégicos que permiten la protección de la información, de los datos personales y de las infraestructuras críticas del Estado, frente a las amenazas que provienen de las interacciones en un Ciberespacio.

Figura 5.

Instancias Especializadas en Ciberseguridad en Colombia.



Fuente: Elaboración propia en Napkin con base en Consejo Nacional de Política Económica y Social (2011). Documento CONPES 3701.

El CONPES 3701 comenzó a ir más allá del aspecto técnico, para consolidar la ciberseguridad y ciberdefensa como aspectos centrales de la seguridad nacional, fortaleciendo el marco normativo y regulatorio como la Ley 527 de 1999, sobre comercio electrónico y firma digital.

Así como, la Ley 599 de 2000, Código Penal, referente a artículos sobre interceptación y violación de la comunicación; la Ley 962 de 2005, uso de tecnología en la gestión pública y, sobre todo, la Ley 1273 de 2009, que modificó el Código Penal, para proteger la información y los datos.

Con el paso del tiempo, se evidenció su limitación frente a los nuevos escenarios de la digitalización, donde los riesgos no solo provenían de ataques externos, sino también de fenómenos internos.

Sin embargo, en el marco de transformación tanto tecnológica como social, el Estado colombiano asumió la necesidad de ir más allá del enfoque de ciberseguridad y plantearse un enfoque más integrador de la seguridad digital, que incluyera no sólo la seguridad de los sistemas informáticos a la hora de interactuar con una población de usuarios, sino que acompañara también la ciberseguridad con la seguridad del usuario, la protección de la información y la protección de los derechos en el Ciberespacio.

Este paso de la ciberseguridad a la seguridad digital quedó oficializado a través del Documento CONPES 3854 de 2016, titulado "*Política Nacional de Seguridad Digita*l", el cual se encargó de reformular la acción nacional a partir de la incorporación de la gestión del riesgo, la confianza en línea, la innovación tecnológica y la cooperación internacional, como ejes de acción básicos para garantizar la mejor resiliencia en un país con estos antecedentes.

La Política Nacional de Seguridad Digital, contenida en el CONPES 3854 de 2016, insiste en la necesidad de gestionar, controlar, mitigar y minimizar los riesgos que son propios de un entorno digital. Este documento complementa y moderniza el CONPES 3701 del año 2011, el cual establecía las bases de la política nacional de ciberseguridad y ciberdefensa.

El texto parte de la constatación del uso masivo y continuo de las Tecnologías de la Información y de las Comunicaciones (TIC) en el país, las que, si bien son un motor de desarrollo, también incrementan vulnerabilidades que deben ser abordadas de una manera global para proteger al ciudadano, al Estado y al sistema económico nacional.

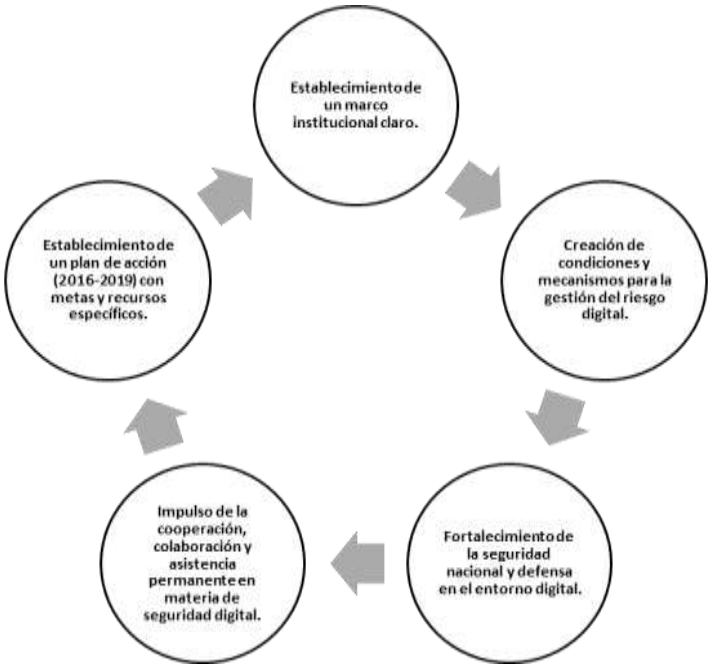
Uno de los ejes sobre los que se centra el CONPES 3854 es la apuesta por un enfoque de gestión de riesgos, entendiendo que el entorno digital es dinámico y que requiere de respuestas continuas y adaptadas.

La política planteada propone fortalecer la capacidad de todos los actores —los participantes del sector público, del sector privado y de la sociedad civil— de manera que sean capaces de identificar, prevenir y mitigar los riesgos inherentes a la seguridad digital en cada una de sus actividades,

En otras palabras, la propuesta busca consolidar una cultura de corresponsabilidad respecto a los retos que plantea la transformación tecnológica, apoyándose en 5 ejes fundamentales.

Figura 6.

Ejes del CONPES 3854 de 2016.



Fuente: Elaboración propia con base en Consejo Nacional de Política Económica y Social (CONPES). (2016). Documento CONPES 3854.

Pese a los avances logrados con los CONPES 3701 de 2011 y 3854 de 2016, en materia de seguridad digital, se mantenía una concepción técnica y reactiva, centrada en la protección de las infraestructuras críticas, la evitación de los ataques informáticos o la coordinación entre las instituciones especializadas y las civiles.

Aunque estos CONPES pueden considerarse un punto de partida, su propuesta queda limitada ante la serie de nuevas problemáticas emergentes como la pandemia COVID-19, la cual, aceleró el tránsito de la cotidianidad material al Ciberespacio de manera abrupta. El entorno virtual se convirtió, pues, en el escenario privilegiado para el desarrollo de todas las actividades laborales, educativas y sociales.

Para Jorge Ivan Contreras Cardeño (2021) dispone que para la vigencia de 2020 "el impacto del COVID-19 supuso un nuevo acelerón en la digitalización de la sociedad, traducido en el crecimiento del uso de internet en general y de las redes sociales en particular" (p.102).

De igual manera**,** Fernando Miro Llinares (2021) "el confinamiento ha acelerado y acelerará la digitalización, que, a su vez ya estaba desplazando al Ciberespacio actividades cotidianas y con ello oportunidades que hacen que aumenten los ciberdelitos*"*(p.12).

Lo anterior, es porque al ser el Ciberespacio una arquitectura abierta, descentralizada y, hasta cierto punto, anónima, genera un ámbito propenso a que varios actores no estatales hagan un uso estratégico, ideológico o criminal de este.

Con la crisis sanitaria y la globalización, las políticas desarrolladas comenzaron a tener lagunas en su actuar frente al nuevo panorama digital que se iba desarrollando, encontrando ausencia de una gobernanza jurídica tanto interna, como global, convirtiéndose en una amenaza más ofensiva para los Estados por las características que le son propias.

La fragilidad estructural del espacio digital y la falta de una regulación global efectiva han sido ocupadas en la actualidad por aquellos que hacen un uso de la tecnología con fines ilegales o violentos. Así aparece el Terrorismo Digital (TDig); una forma actual de amenaza, asociada a la

utilización del Ciberespacio en su componente digital como instrumento fidedigno de coerción, intimidación o desestabilización.

Esta forma de terrorismo no sustituye al terrorismo tradicional; lo complejiza, a través de nuevas modalidades de ataque que se deslizan con fluidez entre fronteras y que son llevados a cabo desde la supuesta invisibilidad del componente virtual.

Desde esta óptica, el Ciberespacio como nuevo fenómeno ha cambiado radicalmente la naturaleza de las amenazas terroristas, debido a que los actores ya no se limitan a los métodos tradicionales de violencia física, sino que ahora operan de manera virtual, facilitando la expansión de su ideología y acciones a un público más amplio y sin las restricciones geográficas que podrían haber existido antes.

Si bien, no existe un desplazamiento de la delincuencia hacia el Ciberespacio-ya que este no sustituye la realidad física- sí puede afirmarse que lo complementa o la amplía, generando nuevas dinámicas para la composición de conductas punibles, pues lo actores al detectar nuevas oportunidades con menor riesgo, diversificaron su portafolio criminal; por lo que el crimen no migra sino se adapta.

En opinión de Fernando Miró Llinares (2021) “los cibercriminales, cambian los objetivos, los medios o tácticas para su ejecución, los tipos de infracción o, incluso, la identidad virtual o «ciberlugar» desde donde se realiza el ataque ”(p.9*),* por lo que los delincuentes, en este nuevo marco, reinterpretan el crimen a partir de las dinámicas del espacio virtual: anonimato, descentralización, su dimensión global, su inmediatez.

Tabla 5.

Adaptación del crimen al Ciberespacio.

Adaptación tipológica	Los delincuentes responden al bloqueo de un determinado tipo de acto delictivo, cometiendo delitos totalmente diferentes.
Adaptación de objetivo	Los cibercriminales desechan el ataque a objetivos bien protegidos y centran sus esfuerzos en otros más vulnerables.
Adaptación técnica	El cibercriminal mejora su ataque y utiliza nuevos instrumentos para superar las nuevas barreras.
Adaptación de ciberlugar	Los cibercriminales cambian el lugar en el ciberespacio desde el que realizan el ataque o el nombre de la web desde el que actúan criminalmente.

Fuente: Tomada de Llinares, 2021, p. 9

La tabla referenciada evidencia que los criminales no desaparecen frente a las regulaciones tradicionales, sino que adaptan sus tácticas para sacar partido de los beneficios del ambiente digital reconfigurando su actividad.

La adaptación tipológica muestra el reemplazo de delitos físicos por acciones virtuales con un marco jurídico más difuso; la de objetivo, la identificación de víctimas más vulnerables; la técnica, la renovación continua de instrumentos para sobrepasar obstáculos de seguridad; y la ciberlugar, el tránsito entre plataformas con el fin de no ser detectado (Llinares, 2021).

En ese sentido, la evolución de la delincuencia hacia el entorno digital, facilita el entendimiento de cómo las estructuras delictivas se han reorganizado en función de la tecnología. Esta misma lógica de adaptación, a su vez se reproduce en un nivel mucho más complejo con la irrupción del terrorismo en el Ciberespacio, fenómeno que no ha sido ajeno a su implementación.

Bajo este referente, el terrorismo ha mutado profundamente a lo largo del tiempo y en la época contemporánea se ha adaptado de manera clara al Ciberespacio; si bien sus raíces se encontraban ancladas a la acción directa, el terrorismo ha evolucionado a formas más sutiles que encuentran en el Ciberespacio un buen lugar de expansión y aceleradas por la pandemia de COVID-19.

Esta transición no significa que el terrorismo clásico haya desaparecido; significa que ha evolucionado, se ha transformado, permitiendo a al terrorista ampliar su radio de acción hasta el punto de llegar al concepto de una práctica global virtual que redefine su actuar criminal al ofrecer un entono idóneo de rápida difusión y acceso a la información sin necesidad de presencia directa.

Es por ello, que autores como Miguel Ángel Poveda Criado y Begoña Torrente Barredo (2016) en su artículo establecen que el terrorismo, amplia su campo operativo así como transforma su naturaleza en el entorno virtual del Ciberespacio, al tener este unas particularidades propias, dignas de traer a colación:

Figura 7.

Características del entorno digital para el terrorismo.

Fuente: Esquema propio en Napkin con base en Poveda Criado & Torrente Barredo, B. (2016)

Como resultado de ello, existe una adaptación del terrorismo al Ciberespacio que obliga a replantear su conceptualización, que se encuentra arraigada a parámetros tradicionales, para ello se creó la figura del " ciberterrorismo" propuesto en la década de 1980 por Barry Collin, un empleado del Instituto Americano de Seguridad e Inteligencia de California, lo utilizó en el contexto de la transición del terrorismo del mundo físico al virtual, la intersección y fusión de estos dos mundos.

Sin embargo, la complejidad inherente de la conceptualización del terrorismo tradicional se extiende al ámbito digital, por ello, al momento de definir el ciberterrorismo Catherine Theohary y John Rollins (2015) manifestaron lo siguiente:

> Hay varias razones que pueden explicar por qué el término "ciberterrorismo" no ha sido definido legalmente, incluyendo la dificultad para identificar los parámetros de lo que debería considerarse actividades aplicables, si articular líneas rojas claras exigiría una respuesta para incidentes de menor nivel y mantener la maniobrabilidad estratégica para no restringir las actividades futuras de EE. UU. en el Ciberespacio (traducción propia, p. 10).

De esta manera, la ambigüedad es estratégica y obedece al plano internacional del poder imperante, así como frente a posibles incidentes futuros en el Ciberespacio que se conviertan en una amenaza en potencia; por ello, la delimitación rígida de parámetros precisos sobre qué actividades deberían considerarse de carácter meramente terrorista en el entorno digital no permite la maniobrabilidad estatal.

Sin embargo, autores como Dorothy Denning (2000 citada en Poveda Criado & Torrente Barredo, 2016) lo conceptualiza como: *"*Ciberterrorismo es la convergencia entre terrorismo y Ciberespacio. (…) Para calificar como ciberterrorismo, un ataque debe resultar en violencia contra personas o contra la propiedad, o al menos causar el daño suficiente como para generar miedo" (p. 510).

En este contexto, el ciberterrorismo es presentado como un fenómeno online que combina motivaciones ideológicas con medio propios de la ciberdelincuencia trascendiendo los límites

físicos al operar en la red; de tal manera, que se diferencia de otros por su impacto simbólico y psicológico sobre la población; conforme lo establece el autor Saman Iftikhar (2024)

> El ciberterrorismo es el uso deliberado de capacidades cibernéticas, a menudo por actores no estatales, con la intención principal de causar miedo, pánico o disrupción generalizada en una población, gobierno u organización. Los actos de ciberterrorismo típicamente implican ataques motivados política, ideológica o socialmente que tienen como objetivo infraestructuras críticas, resultan en daños significativos o representan una grave amenaza para la seguridad nacional (traducción propia, p.2).

Con ello, el ciberterrorismo congrega todos los elementos propios del terrorismo tradicional su objetivo es generar una desconfianza a gran escala a partir del miedo o el caos en aras de causar daños significativos.

Por ello lo que distingue al ciberterrorismo de otros fenómenos *"*como el cibercrimen o el hacktivismo, es la intención explícita de incitar el terror o desestabilizar sociedades, a menudo en busca de objetivos políticos o ideológicos, en lugar de una mera ganancia financiera o la búsqueda de objetivos sociales o éticos"(Iftikhar, 2024, p.2).

En consecuencia, los elementos constitutivos del terrorismo tradicional siguen reproduciéndose integralmente en el entorno digital, lo único que se transforma es su canal, un nuevo escenario de confrontación simbólica y operativa, pero con el mismo propósito de infundir terror y alterar los cimientos del pacto social. La violencia física se sustituye por la violencia tecnológica como medio para extender sus fronteras territoriales.

Figura 8.

Elementos conceptuales del ciberterrorismo.

Fuente: Esquema propio.

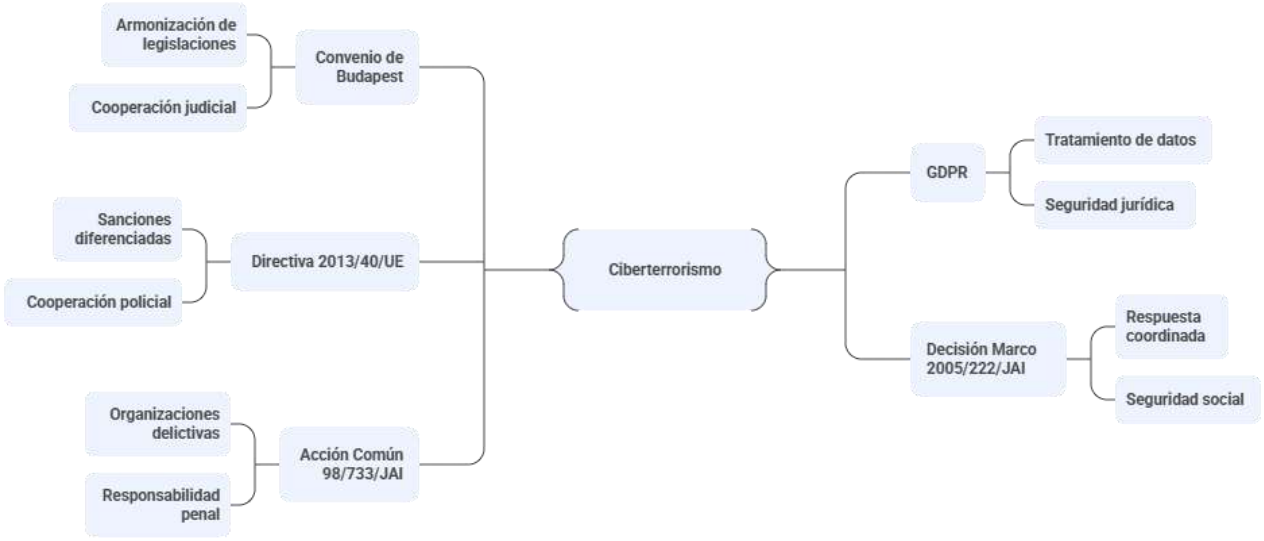
La violencia tecnológica, reemplaza la acción directa, al gestionarse desde el uso dañino de las Tecnología de la Información y las Comunicaciones (TIC) ya sea para ejercer poder, control,,terror por medio de "herramientas, equipos, programas informáticos, aplicaciones, redes y medios; que permiten la compilación, procesamiento, almacenamiento, transmisión de información como: voz, datos, texto, video e imágenes"(Art. 6 Ley 1341 de 2009) a la población en general o parte de ella.

Por consiguiente, se abre en la era contemporánea un medio inmaterial, intangible que puede generar daños equiparables o incluso superiores a un atentado físico; en vista de que, puede paralizar un sistema informático, sembrar miedo colectivo, manipular infraestructuras críticas, entre otros aspectos.

Según, Sánchez et al (2024) sostienen que en el ámbito internacional la regulación del ciberterrorismo no es expresa, por el contrario debe dirigirse al tratamiento de la ciberdelincuencia que tiene por finalidad "proteger adecuadamente el nuevo bien jurídico de la seguridad de los datos, la información y las funciones de los sistemas informáticos"(p. 353).

Figura 9.

Marco Normativo Internacional del Ciberterrorismo.



Fuente: Elaboración propia en Napkin con base en Sánchez et al (2024)

A pesar que los avances normativos internacionales, en el campo de la ciberdelincuencia han sido significativos, el desarrollo jurídico del ciberterrorismo sigue siendo escaso y limitado, en la mayoría de los instrumentos, incluido el Convenio de Budapest (2001) y las recientes Directivas Europeas abordan estas conductas bajo la categoría general de delitos informáticos, sin establecer una definición o tratamiento penal específico para los actos terroristas cometidos en el entorno digital.

De igual manera, el ciberterrorismo constituye una de las expresiones más sofisticadas de la criminalidad, pues afecta a una pluralidad de bienes jurídicos (macro-micro). Desde la perspectiva macro, comprende la Defensa y Seguridad Nacional ya que atenta contra la propia soberanía, la estabilidad de la política o la infraestructura estratégica de los Estados.

Ahora, desde la perspectiva de la micro vulnera derechos fundamentales como, por ejemplo: el derecho a la privacidad, a la integridad personal o la protección de datos erosionando la confianza ciudadana en las instituciones y en la tecnología (Sánchez et al 2024).

Razón por la cual, la ciberdelincuencia, que tiene como meta un beneficio, la obtención de información, o afectar de alguna forma un sistema informático para objetivos particulares; difiere del ciberterrorismo, pues este tiene la finalidad de causar miedo, llevar a la inestabilidad de instituciones, producir caos social o político, o atentar contra la integridad del Estado o de las comunidades aledañas dentro de este.

En virtud de ello, la regulación del ciberterrorismo no puede basarse en la regulación de la ciberdelincuencia ya que involucra la salvaguarda del orden público, la defensa nacional y la protección de la ciudadanía frente a amenazas organizadas que utilizan medios tecnológicos para fines terroristas, es decir obedece al bien jurídico de la seguridad pública.

2.1.4. El Terrorismo Digital y su distinción con el terrorismo tradicional.

Ahora bien, conviene resaltar, que el ciberterrorismo al ser un fenómeno de naturaleza compleja presenta múltiples definiciones a causa de su amplio espectro de manifestaciones; por lo tanto, resulta pertinente establecer una categorización que delimite su alcance; considerando que existen numerosas formas de su accionar que obedecen a distintos niveles de afectación de seguridad pública

La exigencia de la delimitación, obedece a que las Tecnologías de la Información y de las Comunicaciones (TIC) son un espacio amplio, que integra: la difusión instantánea de información, la interferencia de infraestructuras críticas, la manipulación de datos y la creación de miedo comunitario a través de la manera virtual

Para ello, se trae a colación la clasificación de los delitos cibernéticos como punto de referencia para establecer dicha diferenciación.

Los delitos que se desarrollan en el Ciberespacio comprenden dos categorías esenciales desarrolladas por la doctrina de David Wall (2007) y Peter Grabosky (2001); pero de manera formal por el Ministerio del Reino Unido (Home Office) en su informe *Cybercrime: A Review of the Evidence* (2013), recogida por la INTERPOL en su documento *National Cybercrime Strategy Guidebook* (2021), donde retoma la siguiente clasificación:

Tabla 6.

Tipología de Delitos en el Ciberespacio.

Característica	Delitos Cibernéticos Dependientes	Delitos Habilitados por la Tecnología
Dependencia Tecnológica	Esencial para la comisión del delito	Facilita la comisión del delito
Tipo de Delito	Delitos nuevos, específicos de la tecnología	Adaptaciones de delitos preexistentes
Objetivo	Sistema informático, red o datos	Víctimas, bienes o servicios
Escala	Limitada por la infraestructura cibernética	Ampliada por el alcance de la tecnología
Ejemplos	Sabotaje cibernético, hacking, malware	Fraude en línea, ciberacoso, contenido ilegal
Implicaciones	Amenaza a la seguridad, pérdidas económicas	Mayor alcance, dificultad en la investigación

Fuente: Elaboración propia en Napkin con base en INTERPOL (2021).

En el marco de los delitos cibernéticos, como se observa, existen dos dimensiones: los cibernéticos dependientes *(Cyber-dependent crimes*) los cuales comprenden el uso directo de sistemas informáticos –del tipo del sabotaje cibernético– como ataques a redes o infraestructuras críticas.

Así como, los delitos habilitados por la tecnología (*Cyber- enabled crimes*), aquellos que sacan partido de la tecnología como las redes para facilitar determinadas conductas preexistentes en el ordenamiento jurídico penal.

A partir de esta dualidad, el terrorismo se abre a adoptar expresiones que le son propias de la cibercriminalidad, por lo tanto se tiene que el ciberterrorismo posee dos vertientes: El terrorismo informático y el Terrorismo Digital (TDig).

Bajo esta tipología, el componente técnico es el núcleo de la delimitación, pues, se distinguen en aquellos terroristas que emplean la tecnología como medio y aquellos que la convierten en un fin en sí mismo:

Figura 10.

Tipos de Ciberterrorismo

Fuente: Elaboración propia en Napkin con base en INTERPOL (2021).

Atendiendo a la tipología del delito cibernético se desarrolla el ciberterrorismo, se propone esta clasificación conceptual con la finalidad de delimitar con mayor precisión el uso dañino de las TIC bajo dos dimensiones.

Por consiguiente, el terrorismo informático comprende el uso directo de tecnologías digitales, derivado de los ataques cibernéticos o de la guerra cibernética; ya que se puede pensar en el mismo como el uso de técnicas informáticas y de herramientas para atacar sistemas informáticos, redes o infraestructuras digitales, produciendo daños técnicos.

Figura 11.

Manifestaciones del Terrorismo Informático

Fuente: Elaboración propia en Napkin con base en Poveda Criado, M & Torrente Barredo, B. (2016).

La violencia tecnológica se delimita en el uso directo de las TIC como arma de ataque, orientada a generar dañaos materiales a infraestructuras informáticas, sustituyendo la agresión de construcciones o edificios, por la agresión informática, de manera instrumental, mediante la interrupción de sistemas y flujos de información con el fin de generar colapso o desconfianza en la seguridad pública.

En cambio, el Terrorismo Digital (TDig), engloba aquellos delitos tradicionales que se ven potenciados gracias a las nuevas herramientas tecnológicas, no busca un daño técnico, busca

utilizar canales digitales como el internet, plataformas virtuales “para difundir propaganda, recaudar fondos y blanquear dinero, reclutar y entrenar miembros, comunicarse y conspirar y lanzar ataques mientras los gobiernos intentan contrarrestarlos y atraparlos utilizando medios tradicionales”(Weimann, 2006, traducción propia p. 6)

El Terrorismo Digital a partir de ahora TDig, no necesita necesariamente de armas convencionales o de la ocupación física de un lugar, sino la apropiación simbólica y control estratégico de la circulación de información, la manipulación psicológica de las masas, la desestabilización social generada por campañas de desinformación, e incluso la propaganda radical son suficientes para ocasionar caos, inseguridad o presión política.

Por tanto, no solo supone la incorporación de una nueva herramienta de ataque al repertorio de las formas de terrorismo que ya se conocían, se convierte en una variante del mismo completamente adaptada a las lógicas de un mundo mediatizado por los algoritmos, las plataformas y las redes sociales; de allí que sea transnacional.

Para el TDig, el control de la información y la influencia de las masas es vital para su desarrollo, convirtiéndose en armas más letales que los propios explosivos, bien lo decía Manuel Castells (2009), en la sociedad-de la información *“*el poder reside en la capacidad de construir significados compartidos en los flujos de comunicación”(p.10) y justamente ahí radica su fuerza.

La batalla no se efectúa con armas ordinarias, ni tampoco en espacios geográficos con límites concretos, sino que ahora tiene lugar en el Ciberespacio, donde la gran red (internet) y las plataformas sociales representan el ámbito del escenario del conflicto.

El clima del internet es tan fructífero que según Thomas Timothy (2003), es perfecto para que un grupo radical explique sus acciones o contrarreste la condena tanto interna como internacional, especialmente al utilizar servidores específicos. Internet puede atacar tanto a indecisos como a creyentes con diferentes mensajes, orientados a su público objetivo.

De igual manera, autores como Sara Zeiger y Joseph Gyte (2020) expresan que los miembros de los grupos terroristas contemporáneos han crecido con la implementación de la

tecnología y con ello con el acceso a internet y redes sociales; circunstancia que explica porque en la actualidad estas plataformas desempeñan un papel fundamental en su accionar delictivo.

Si bien, las redes sociales, foros, blogs, webs han tomado iniciativa en aras de generar reglamentos que le faciliten la no tolerancia frente a organizaciones terroristas, siguen siendo espacios de escaso control jurídico y social; e incluso al comenzar a delimitar este campo, las células terroristas encuentran en la Deep Web y en el segmento de la Dark Web un medio idóneo para continuar con sus actividades ilegales de manera clandestina y sin ningún tipo de rastro.

Según Alfredo, Zechlinski y Fonseca (2024)

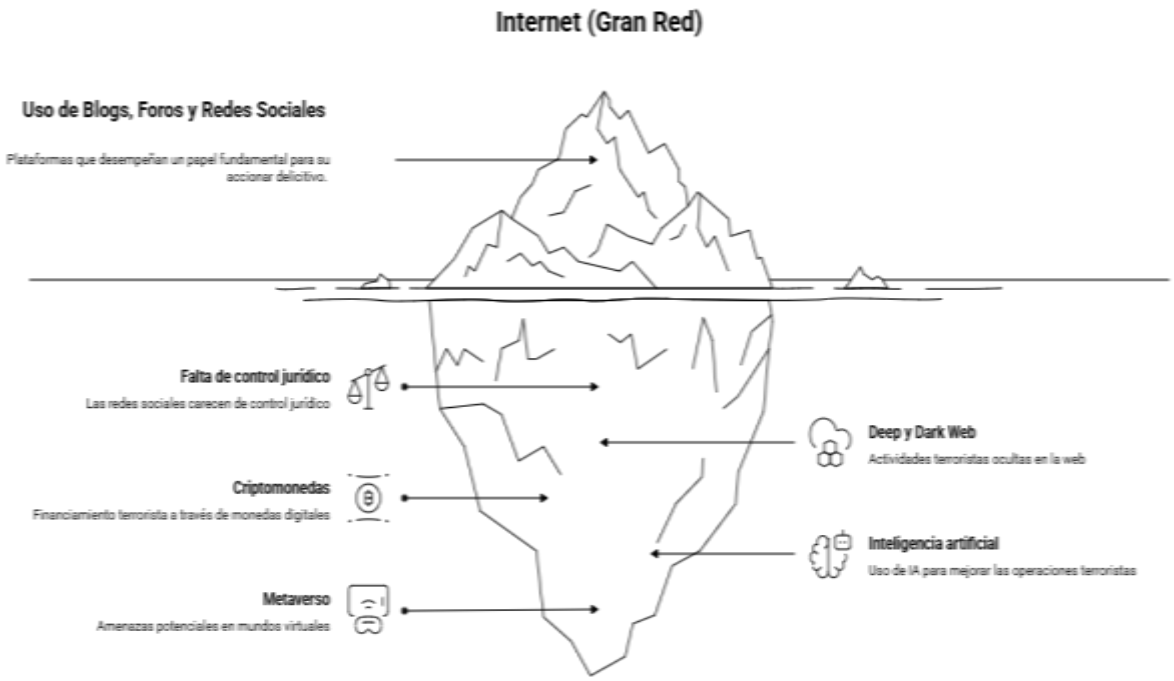
> Si bien internet impulsa las interacciones remotas de una manera sin precedentes y, en consecuencia, genera un aumento exponencial en el acceso y la creación de contenido digital, también existe una intensa competencia por la atención y la participación de los usuarios, concentrada en un conjunto restringido de plataformas, sitios web y aplicaciones (p.37)

No obstante, no son los únicos escenarios, el uso de criptomonedas para su financiamiento, la utilización de inteligencia artificial para hacer más efectivo su actuar, e incluso el metaverso se convierte en amenazas potenciales.

Personajes como Samar Violeta Francisco Agra (2022) han ido expresando su verdadera preocupación, en aquellos espacios que poseen una inmersión digital como el metaverso, porque si bien, puede realizarse estrategias intrínsecas de su actuar, poco se habla de la repercusión psicológica de un ataque en dicho espacio.

Figura 12.

Medios del Terrorismo Digital.



Fuente: Elaboración propia en Napkin con base en Francisco Agra, S. V. (2022)

Con esto en mente, los terroristas intentan hacerse con la atención, con el discurso, e incluso con las emociones de la opinión pública y en tal sentido la información y la tecnología se convierten en medios de coerción ideológica.

El paso a lo cibernético convierte el acto terrorista en un medio para la influencia de un todo, el de una estrategia de efectos globales, una estrategia de influencia capaz de extenderse en el tiempo y en el espacio.

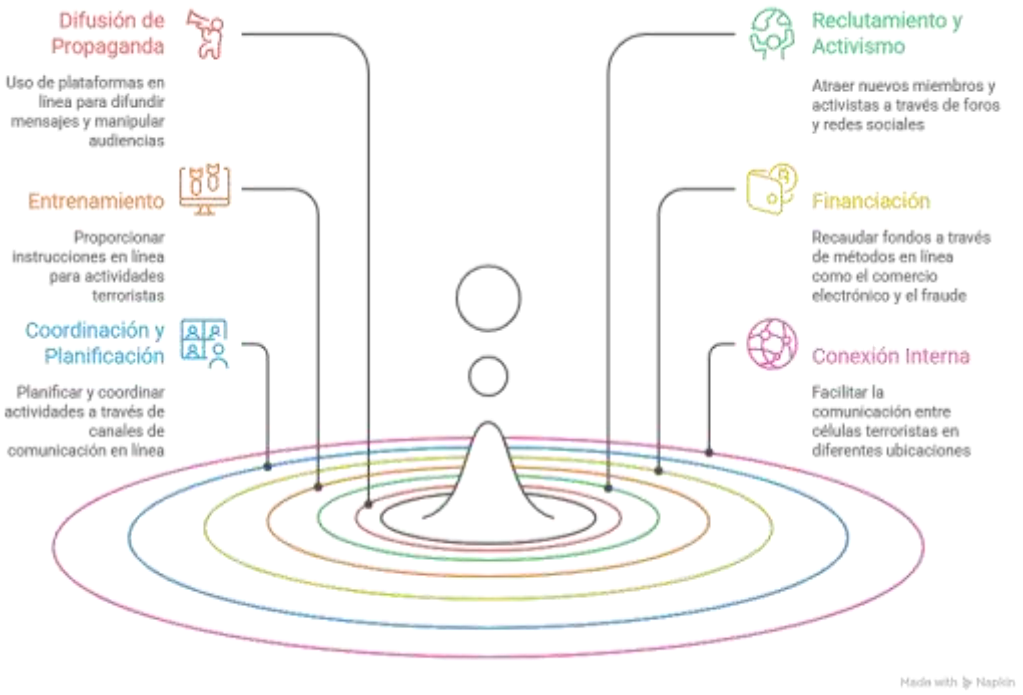
La instrumentalización del entorno digital para facilitar sus prácticas ilícitas, incrementa su impacto. De ahí, que el TDig presente un conjunto de estrategias que, desplegadas en el ámbito virtual, van destinadas a provocar miedo, segmentar a la sociedad, desgastar a las estructuras

estatales, así como a imponer y dar cauce a unas ideologías extremistas y todo ello sin necesidad de violencia física directa.

El desarrollo de estas estrategias a través de canalizaciones digitales puede caracterizarse por un carácter flexible, anónimo y apto para generar efectos simbólicos y políticos de gran proyección, su materialización en el Ciberespacio se encuentra desarrollado por un actuar común:

Figura 13.

Estrategias que desarrolla el Terrorismo Digital.



Fuente: Elaboración propia en Napkin con base en Poveda Criado, M. & Torrente Barredo, B. (2016).

De este modo, la facilidad del internet ha logrado edificar todo un ecosistema integral de operatividad ilícita eficaz para los actores terroristas, otorgando un alcance a escala global sin precedentes, que desafía los marcos jurídicos actuales y los límites generados por el derecho internacional público y Derecho Penal internacional.

Vale la pena destacar que, la propaganda y el reclutamiento adquieren una nueva dimensión a través de las redes sociales, mientras que la financiación digital permite el flujo de recursos sin rastreo efectivo. Asimismo, los espacios virtuales de entrenamiento y las plataformas cifradas para la planificación evidencian una profesionalización técnica que trasciende fronteras, en conjunto con la conexión de células terroristas.

Las estrategias comentadas, convergen en ser un campo extenso que ha sido ampliamente abordado por distintos doctrinantes en especial la Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC) por ser una amenaza de gran impacto a nivel trasnacional ya que, su básica asimetría, anonimato y bajo coste lo convierten en especial peligro para los Estados modernos.

Hecha esta salvedad, la violencia tecnológica del TDig, se manifiesta en el plano comunicacional o simbólico de las TIC, es decir a través de la gran red, que contempla: redes sociales, plataformas de comunicación, videos, foros, entre otros; aprovechando la difusión instantánea de la información y la vulnerabilidad emocional de las audiencias.

En virtud de ello, la finalidad del TDig se dirige a afectar a la población civil en general, a la opinión pública e incluso la estabilidad política por medio de plataformas que expenden la influencia de los grupos terroristas más allá de su capacidad operativa real, por las estrategias adoptadas en ella, sembrando terror, odio o polarización en la sociedad mediante el uso estratégico de los recursos tecnológicos..

Con todo el TDig se define como una derivación del ciberterrorismo por cuanto su forma de violencia tecnológica se encuentra en el plano comunicacional de las TIC: usando redes, plataformas y medios digitales.

En aras de difundir miedo, odio o desinformación, con el fin de afectar a la población civil o parte de ella, manipular la opinión pública y desestabilizar la estabilidad social o política; ya que socava de manera silenciosa los propios pilares del orden democrático la confianza y la seguridad digital derivada de la seguridad pública.

En efecto, el TDig se configura como una amenaza directa al bien jurídico de la seguridad digital, concebida como una manifestaciones la seguridad pública, en tanto busca salvaguardar a la población frente a actos dañinos para el pacto social, mediante el uso indebido de las TIC bajo el marco comunicacional digital (no físico, no técnico).

Para finalizar, la comunidad internacional continúa el desarrollo de tratados, convenciones internacionales para el fortalecimiento de la lucha contra el terrorismo; sin embargo, para la época no ha sido elaborado un tratado/convenio internacional específico para el ciberterrorismo.

Si bien, sí existe un reconocimiento pleno de la amenaza que constituyen las Tecnologías de la Información y la Comunicación (TIC) en los actos terroristas, no se encuentra como prioridad dentro de la agenda, por cuanto todo se deja al margen de la cooperación internacional y normatividad interna.

La mayoría de convenciones, como la Convención Interamericana contra el Terrorismo (2002) de la OEA, o las resoluciones del Consejo de Seguridad de la ONU, continúan el desarrollo de un terrorismo tradicional, en conjunto con otros instrumentos internacionales referenciados en todo el apartado. Poco se habla de la prioridad de guiar a nivel global las actuaciones ilícitas que excedan el pacto social.

El propósito de Derecho Penal internacional se ve obstaculizado conforme avanzan las estrategias empleadas por los grupos terroristas, sumado a la incapacidad técnica e institucional de la comunidad internacional, para hacer frente de manera ostensible a este dilema.

En conclusión, la evolución del terrorismo al Ciberespacio evidencia una profunda transformación las nuevas dinámicas delictivas contemporáneos, donde la violencia digital, es el medio instrumental por excelencia; bajo este contexto se presenta el TDig como nueva amenaza desafiando los límites del poder punitivo y la capacidad del Derecho Penal internacional para salvaguardar la seguridad digital como bien jurídico a proteger.

Esta circunstancia permite ineludiblemente reflexionar acerca de los modelos de respuesta penal ante situaciones extremas que sobrepasan las fronteras físicas y jurídicas tradicionales.

2.2 Capítulo II. El Derecho Penal del Enemigo: Fundamentos Teóricos en la Obra de Günther Jakobs.

2.2.1. Del funcionalismo normativista al Derecho Penal del Enemigo: regulación y control frente a amenazas extremas.

Aristóteles exponía desde una dimensión socio-política que el ser humano es por naturaleza un ser zoon politikon, esto sugiere que la especie está predispuesta a la sociabilidad y encontrar su bienestar a través de los otros.

En consecuencia, el ser humano, no es un ente aislado, por el contrario la realización de su propia naturaleza emerge de la participación activa de la vida colectiva, en el cumplimiento de sus deberes o la responsabilidad compartida. Su identidad se encuentra en constante conexión con la contribución del bienestar común y el rol que desarrolla en la sociedad en la que se desenvuelve.

El cuerpo humano, de manera análoga se constituye de diversos órganos que se complementan para el correcto funcionamiento, lo mismo pasa con la sociedad, "el buen funcionamiento de la sociedad y la perdurabilidad de la misma, se determina por la cohesión, sincronización y correcto funcionamiento entre sus estructuras u órganos"(Arias, 2017, p.3).

De allí, que la sociedad no es un conjunto de individuos, sino un sistema organizado que permite la supervivencia de la especie a través de la cooperación e intercambio entre los individuos, siendo previsible su constante interacción. Esta interdependencia converge en una serie de reglas comunes que regulan el comportamiento y aseguran la convivencia colectiva.

La sociabilidad del ser humano posibilita la formación de estructuras sociales complejas- instituciones- que buscan regular su comportamiento dentro de un conglomerado. No obstante, dentro de su naturaleza es innato el conflicto entre iguales (como hecho social consustancial) que

ha generado en distintos tiempos históricos transformaciones de gran relevancia para la evolución de la especie.

El antagonismo social, es una invariable que puede presentarse en diversos ámbitos y en la que la comunidad ha reparado diseñando mecanismo de control y sanción que regulan conductas desviadas, protegiendo así su pacto social.

En este contexto, el funcionalismo, surge como una corriente sociológica que se construye en la comprensión de las estructuras sociales desde un análisis de sus funciones o segmentos específicos de él, abandonando su génesis histórica, extendiéndose a otras disciplinas como la psicología, la política y el derecho (Montoro, 2007).

Desde esta perspectiva, exponentes como Emile Durkheim, ven a la sociedad como un sistema integrado donde cada institución cumple funciones claras para mantener el orden social, pese a las tensiones internas. Esta visión fue profundizada en mayor medida por Talcott Parsons al extenderla a instituciones no solo como la familia, educación, economía, religión; sino también desde la política y el derecho.

El arribo del funcionalismo al derecho, en especial al Derecho Penal, fue un proceso gradual; en principio, Talcott Parsons estableció una línea de pensamiento, donde el derecho es una institución social fundamental al cumplir una función reguladora que garantiza cooperación y control social.

Claus Roxin, toma esta idea, e intenta servirse de ella para dejar así la ardua disputa entre escuelas penalistas (causalista- finalistas) de la Alemania de los años 60, dado que buscaba superar el formalismo y positivismo de la dogmática penal para acercarla a la realidad social. “Es decir, hasta el momento dogmática y realidad se encontraban ubicadas en planos distintos e incomunicados y en no pocas ocasiones las soluciones dogmáticas —adoptadas al margen de la

realidad social— producían resultados insatisfactorios desde una perspectiva práctica"(Arias, 2006, p.440).

Roxin, en su obra *"Política criminal y sistema del Derecho Penal"* (1963), sostiene que el Derecho Penal no debe analizarse siempre desde una estructura dogmática, sino desde la función que cumple dentro de la sociedad, para ello se enfoca en los fines político-criminales del Estado de Derecho, unificando tres ámbitos: política criminal, dogmática penal y fines de la pena; logrando así un funcionalismo teleológico.

De este modo, la dogmática debe interpretarse a la luz de la función que cumple dentro del sistema penal, no a limitarse a describir estructuras del delito. La dogmática penal, no es una esfera autónoma debe servir a la política criminal que fija los fines sociales que debe perseguir el Derecho Penal, estos son: la protección de bienes jurídicos y la preservación como última ratio del orden social.

Por consiguiente, el bien jurídico aparece como eje central de su teoría pues, está conectado al sistema social, al concebirse como "aquello que resulte útil para el desarrollo del individuo o para el propio sistema social, de suerte que su concepción material de lo injusto será precisamente la lesión de esos bienes útiles para el individuo o para el sistema"(Arias, 2006, p.441).

Su postura deviene, en un sistema abierto, por lo que el delito es visto desde dos dimensiones: la categoría dogmática que lo compone y si esa conducta es lesiva para los bienes jurídicos del sistema social. Dicha lesión, comporta la activación de un sistema jurídico punitivo alejado de la retribución sino enfocado en la prevención.

Como se observa, el conflicto es consustancial al ser humano, como las conductas desviadas hacen parte de la sociedad, pues corresponde a la imperfecta naturaleza de la especie, si bien la criminalidad no puede ser erradicada, si puede hacérsele frente con mecanismos racionales

que comprende estrategias no solo jurídicas, también sociales, políticas, económicas; en aras de minimizar los efectos del delito, corrigiendo las causas que motivan la conducta.

En este aspecto, no existe un Derecho Penal que erradique la criminalidad, por el contrario Roxin reconoce que es insuficiente, pero que en su ámbito debe ser interpretado conforme a los fines preventivos utilidad que le da el sistema, el discurso no se encamina a la norma, se encamina al ser humano en sociedad, bajo una estructura donde el Derecho Penal debe limitar su aplicación, pero es necesario para imponer el orden y evitar la anarquía.

En coherencia con su pensamiento garantista, establece que la pena debe aplicarse como medida final, cuando todos los mecanismos de control social fallaron en su intento frente a una conducta desviada, al ser la intervención más severa que tiene el Estado.

La pena, no está dada por la disuasión que deriva del castigo, sino por la necesidad concreta que desarrolla la función preventiva al hacerla imprescindible para la sociedad; lo cual evita que el Derecho Penal se convierta una herramienta de opresión.

Para Roxin, las penas ya son un medio inadecuado frente al criminalidad, porque sigue existiendo tanto el fenómeno como la reincidencia; su análisis establece una crítica dirigida a la penas privativas de la libertad porque si bien son necesarias para delitos graves son inadecuadas para uno de los fines mismo de la pena: la reintegración del individuo a la sociedad, amparado bajo la idea de que el ser humano es un hombre social y apartarlo de ella, comporta mantenerlo en la conducta desviada.

Roxin prueba que la prisión, en muchos casos, corta los lazos sociales que pueden tener un efecto positivo en la reinserción y da lugar a efectos criminógenos, principalmente considerando las penas cortas.

En vez de prevenir la criminalidad, la cárcel puede ser el punto de partida de la carrera criminal, replicando la misma conducta que se desea eliminar; por eso su propuesta es una sustitución gradual de las penas de prisión por otras medidas que sean menos lesivas y más eficaces como medidas preventivas (Arias, 2006).

Figura 14.

Estrategias del enfoque preventivo de Claus Roxin.

Fuente: Elaboración propia en Napkin con base en (Arias, 2006)

El funcionalismo teleológico roxiniano, apoyado en la concepción de un Derecho Penal al servicio de la sociedad, cuyo seno sea regido por fines de prevención, es el punto de encuentro entre la función y el valor, entre la protección del individuo y la estabilidad del orden social.

Su modelo dogmático se encuentra comprometido con la realidad empírica del delito, pero a la vez acota estos límites axiológicos en un Estado de Derecho.

Sin embargo, es partir de la teoría de los sistemas de Niklas Luhmann, que Gunter Jakobs analiza el funcionalismo en el Derecho Penal, sustituyendo como eje el bien jurídico tutelado a la vigencia del sistema normativo; en este enfoque la pena es mecanismo de reafirmación del orden social, necesario para mantener su legitimidad y funcionalidad en el entramado social.

Con el funcionalismo sociológico de Niklas Luhmann, se genera una transformación profunda que lo aleja de las concepciones finalistas.

El sociólogo, precisa a la sociedad como un sistema que a su vez converge en una pluralidad de subsistemas orientado a garantizar el desarrollo social bajo la interacción lingüística y de acción, para él "los sistemas son pues medios de comunicación (en ello radica su racionalidad) que aseguran en su ámbito la transmisión de la complejidad reducida realizada por dichos sistemas, según un esquema binario" (Montoro, 2007, p. 368).

Cada subsistema (familia, educación, derecho, etc.) es autónomo de otras esferas por lo que se caracterizan por la autorreferencia (diferencia entre el sistema y su entorno) y la autopoiesis (producen sus propios elementos).

Lo anterior, permite operar de manera cerrada bajo sus propios flujos de comunicación; con el objetivo, de cumplir una función específica para mantener la estabilidad del conglomerado social, sin que todo dependa de un centro de decisión, pero en constante contacto.

Con la interacción constante de subsistemas, la sociedad se convierte en un sistema complejo, en la que coexisten múltiples interacciones simultáneas que repercuten en un alto nivel de imprevisibilidad del comportamiento del ser humano en sociedad; de ahí que, ante esta imprevisibilidad, el derecho sea un mecanismo destinado a reducirla.

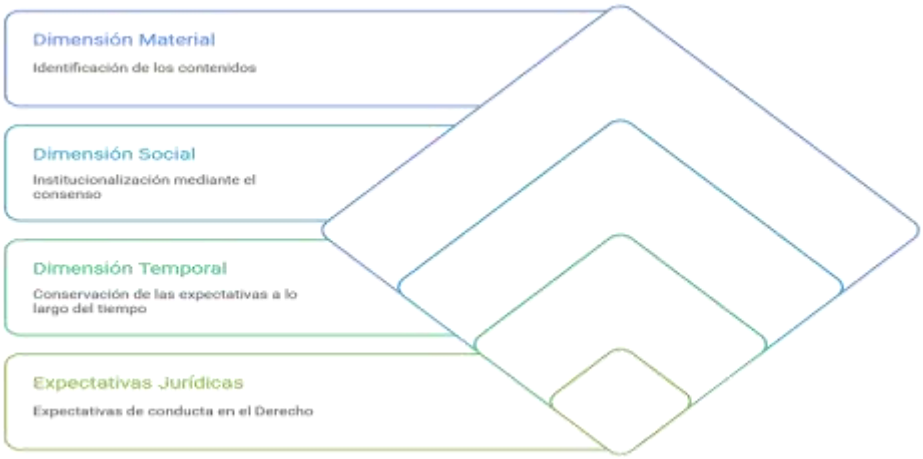
El derecho, es un subsistema encargado de estabilizar las expectativas normativas de los individuos en sociedad. Aunque, no es posible eliminar el conflicto si se torna predecible tratarlo y regular, evitando que se convierta en una amenaza, según el doctrinante Alberto Montoro (2007):

> Luhmann concibe el Derecho como un subsistema específico del complejo sistema social, definido básicamente por la nota de positividad y que se diferencia funcionalmente de los otros subsistemas sociales (económico, moral, político, etc.) por su específico entramado de comunicación consistente en su propio sistema binario -distinción entre lo jurídico (Recht) y lo antijurídico (Unrecht)- capaz de establecer y fijar determinadas "expectativas normativas de conducta"(p. 369).

Luhmann, suprime el elemento humano del derecho y lo convierte en un sistema técnico de comunicaciones normativas, facultando a las personas sobre qué comportamientos son aceptables o no y qué consecuencias tiene obedecer la norma, trayendo consigo previsibilidad normativa, bajo tres dimensiones:

Figura 15.

Dimensiones del sistema jurídico.



Fuente: Elaboración propia en Napkin con base en (Montoro, 2007, p. 369).

Así, el derecho está supeditado a su propio ámbito operativo dentro de la sociedad (ilícito/licito) no a valores metafísicos o morales, sino bajo su propio lenguaje jurídico en su función autorreferencial y autopoiética, al ofrecer normas para reducir la complejidad e incertidumbre que se produce de la convivencia humana.

De este modo, el derecho no se dirige al ser humano, sino al sistema mismo, de hecho muchos críticos como Ignacio Izuzquiza (1989) o Jürgen Habermas (1981), afirman que la teoría de los sistemas produce una "sociedad sin hombres" al ser una visión tan técnica que puede derivar en sistema sociales fríos y despersonalizados, al no validarse con otros sistemas como la moral sino al operar de manera lógica desconecta del entendimiento humano.

Gunter Jakobs, se inspira en esta teoría funcionalista y la adapta al campo del Derecho Penal. Ahora, mientras Luhmann considera a la sociedad como un sistema autopoiético de las comunicaciones, que se reproduce a sí mismo mediante códigos binarios; Jakobs realiza el mismo desplazamiento al campo del Derecho Penal, donde el código funcional se ve expresado como conducta conforme al derecho /conducta que se aparta del derecho.

Su concepción del Derecho Penal, es exclusiva del ámbito objetivo que genera el sistema social, por ello, no se reduce a normas que buscan castigar conductas desviadas, sino por el contrario es un mecanismo funcional que mantiene la cohesión social al garantizar la vigencia de la norma y con ello la continuidad del sistema.

El funcionalismo de Jakobs no es teleológico, es sistemático. Las relaciones sociales de los individuos deben orientarse en base a regularidades previsibles, que establecen las normas legales, las cuales, generan confianza y permiten que haya contacto social sin miedo a consecuencias inesperadas; como resultado de ello, "la identidad de la sociedad se determina por medio de las reglas de la configuración, es decir, por medio de normas y no por determinados estados o bienes"(Jakobs G, 1996, p. 26).

En ese sentido, se concibe a la sociedad como un sistema de expectativas normativas que busca su solidez mediante la previsibilidad de la conducta.

En consideración, su obra *"Sociedad, norma y persona en la teoría de un Derecho Penal funcional*" (1996), las personas desempeñan distintos roles sociales que son a su vez posiciones normativas que los individuos ocupan para que el sistema opere de manera ordenada y adecuada, dentro de distintos ámbitos delimitados por el derecho.

Cuando Jakobs manifiesta que "una sociedad existe cuando está vigente al menos una norma", está afirmando que la sociedad sólo puede existir si las personas comparten expectativas de comportamiento estables y al hacer referencia a la norma, esta "debe entenderse como la expectativa de que una persona, en una situación y circunstancia determinada, se comportará de una manera determinada, sólo y exclusivamente debido a su Ser-Persona" (Montero, 2008, p.17)

De acuerdo con ello, cada uno de los individuos que actúan dentro de la estructura normativa tiene asignado un papel, o actividades dentro de una relación social, que va contribuyendo a la conservación del orden jurídico.

Ahora, cuando un sujeto desempeña correctamente un papel (ciudadano, autoridad o trabajador), está contribuyendo, al mismo tiempo, a la consolidación de ciertas expectativas normativas que son necesarias para el funcionamiento correcto y ordenado del sistema; por el contrario, cuando el sujeto no cumple su papel, se destruyen las expectativas sociales y se pone en peligro la continuidad de ese mismo sistema normativo.

La persona que abandona el rol dentro del sistema activa el Derecho Penal, pues su función se dirige a restablecer el equilibrio afectado, de lo contrario el sistema corre el riesgo de verse fragmentado, por lo que el delito no es la lesión de un bien jurídico, como lo establece Roxin; *"el delito es –comunicación defectuosa es– defraudación de expectativas-"*(Jakobs G, 1996, p. 18) que pone en peligro el orden social, al no actuar de manera previsible como la norma lo exige.

El delito, rompe la confianza que el sistema prevé en los individuos, no hay un contenido moral ni se mide por el daño causado, sino por el impacto que tiene sobre la norma que le da estabilidad al sistema.

De esta forma, se explica por qué para Jakobs el delito es un fenómeno eminentemente funcional, nunca ontológico y tampoco moral ya que la gravedad del delito depende de su potencialidad para alterar la autopoiesis del sistema, en otras palabras, su manera de hacerse operativo y coherente.

La pena por tanto no se encausa a sus fines, busca restaurar la vigencia de la norma que ha sido negada por el individuo en su conducta contraria a derecho; esto es, el Estado en el ejercicio del ius puniendi comunica públicamente que la norma sigue siendo válida, que el orden social no ha sido quebrantado de manera significativa, por lo que las personas pueden seguir confiando en él. "En esta concepción, la pena no es tan sólo un medio para mantener la identidad social, sino que ya constituye ese mantenimiento mismo" (Jakobs G, 1996, p. 18).

De acuerdo, con el doctrinante Alejandro Sánchez González (2009) estima que para Jakobs la pena es una respuesta institucional ante la infracción de una norma "y, mediante ella, se pone de manifiesto que ha de conservársela fidelidad al derecho, a consta del infractor responsable. De esta forma, la misión de la pena consiste en el mantenimiento de la norma, como modelo de orientación para los contactos sociales" (p.199)

En resumen, el delito significa una comunicación negativa-un mensaje en el que se afirma que la norma pudiera haber dejado de estar vigente- y la pena es la comunicación simbólica que se establece desde el sistema jurídico; con la finalidad, de seguir de alguna manera ese mensaje, reafirmando que las reglas continúan siendo de obligatorio cumplimiento.

La misión del Derecho Penal se circunscribe ´precisamente en la prevención general positiva, porque busca reforzar la fidelidad de la norma y no en disuadir al infractor; con ello, si el Derecho Penal únicamente tuviera como finalidad mantener el consenso y reafirmar las normas

sociales, acabaría siendo un instrumento de control social total más orientado a la preservación del orden existente, imposibilitando incluso la transformación social.

Por consiguiente, para Manuel José Arias Eibe (2006) la misión del Derecho Penal es:

> (...)velar por la subsistencia de tales normas y, por tanto, de velar por la misma subsistencia de la sociedad que se apoya en ellas y del orden social conformado, de lo que deriva, en última instancia y de forma mediata, que la identidad y carácter de los mismos individuos, como personas, también resultaron preservados por el Derecho Penal y ello en la medida en que si la sociedad resulta protegida por el Derecho Penal, también lo serán éstos, que sin la misma, serían simples animales.

De esta manera, quien actúa contra el Derecho no solo infringe una norma sino que, además, quiebra el compromiso comunicativo dentro del sistema jurídico-social; por lo tanto, el autor del delito deja de actuar como una persona que da confianza normativa y comienza a ser considerado como un peligro para la estructura de las expectativas colectivas.

Bajo el funcionalismo sistémico o radical, es el ordenamiento jurídico, el que dota al ser humano de su carácter de persona y solo se es persona cuando cumple un rol determinado por la norma social, de lo contrario perdería su estatus de sujeto de derechos y deberes, quedando reducido a su mera existencia biológica.

De esta manera "para el funcionalismo sistémico el concepto de persona está ligado al cumplimiento de la norma, como resultado de la función y rol que este cumple en el ámbito social" (Torres Vásquez, Tirado Acero & Trujillo Florián, 2018, p. 185).

Razón por la cual, la criminalidad está dada por negar la validez del rol que el individuo ocupa en sociedad, o incluso se concibe como una ruptura comunicativa que amenaza la continuidad del sistema.

Al igual que Luhmann, el individuo no es lo importante, sino el comportamiento que de él se despliega en relación con la vigencia de la norma. "De esta suerte, cada uno de los sujetos que

conforman la sociedad son garantes de que las expectativas existentes acerca de ellos no se vean frustrada" (Arias, 2006,p. 447)

Se es persona, conforme se sirva a la sociedad no por su condición humana. Con todo, es la norma la que reconoce al individuo como persona y para ello exige una contraprestación mínima que es la manifestación cognitiva de su voluntad de comportarse conforme a las reglas sociales.

Cuando, la norma desaparece o cuando el sujeto la niega expresamente, el Derecho Penal ya no carga con la estructura de una reafirmación del orden normativo, sino que pasa a convertirse en un instrumento de defensa frente a un enemigo (Sánchez, 2009).

Torres Vásquez, Tirado Acero y Trujillo Florián (2018) sostienen que:

> Se genera un proceso de diferenciación de los individuos en ciudadanos –personas– y enemigos –categoría que implica la pérdida de dignidad, derechos y el mismo estatus de humanidad–, situación que obedece a la necesidad sistémica de inmunidad por medio de preceptos sociales que deben dominar o prevalecer en la conducta de los asociados con la finalidad de mantener el orden establecido. El funcionalismo genera un criterio de división de los individuos, en el cual solo merece un trato digno quien es capaz de asumir su rol social. Nace el concepto «Derecho Penal de enemigo» como resultado de esta distinción (p. 185).

Ante esta dicotomía, Jakobs distingue dos tipos de Derecho Penal: el de los ciudadanos, en el que la sanción pretende ratificar la eficacia de la norma para infracciones esporádicas proporcionales y acordes con el Derecho Penal clásico; pero, no en todos los supuestos.

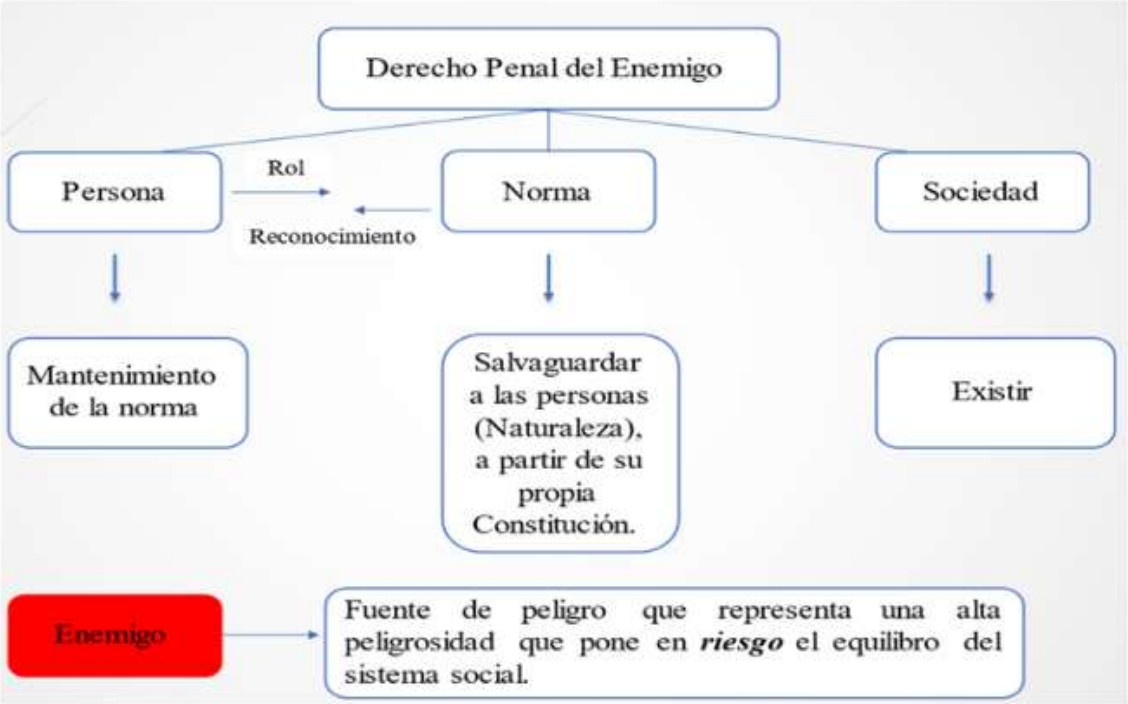
Jakobs pone de manifiesto que esta lógica no puede reconducirse a todo supuesto; ya que, cuando el sujeto niega de forma consciente y persistente el carácter normativo que tiene el orden normativo, deja de ofrecer la certeza cognitiva de que se comporta como persona.

De presentar tal situación, el sistema ya no lo reconoce más como ciudadano, sino como enemigo: un ente que amenaza estructuralmente la existencia del sistema social. "En este sentido

Jakobs estima que "el Derecho Penal de enemigos optimiza la protección de bienes jurídicos, mientras que el Derecho Penal del ciudadano optimiza esferas de libertad"(Sánchez, 2009, p. 200)

Figura 16.

La Sociedad en el funcionalismo normativo del profesor Günther Jakobs.



Fuente: Tomada de (Vásquez, 2022, p.3)

De tal forma que, desde esta óptica, Jakobs llama la atención sobre las situaciones en las que el modelo tradicional del Derecho Penal no logra ser eficiente y con ello, incorpora un nuevo sistema en los sujetos que no pueden ser incluidos dentro del esquema criminal clásico, puesto que su comportamiento no responde a una racionalidad relativa al pacto social.

2.2.2.. Antes de Jakobs: fundamentos filosóficos de la figura del enemigo.

Kai Ambos (2007) dispone en su obra que una de las primeras manifestaciones de la figura del enemigo deriva del filósofo de la antigua Atenas, Aristóteles, en sus escritos como "*Ética a Nicómaco*" al escribir sobre el Estado, particularmente en tiempos de conquista y conflictos bélicos, comienza a forjar la conceptualización del enemigo desde dos perspectivas: el enemigo externo y el enemigo interno.

Para Aristóteles, la polis no es un mero territorio, sino que se encuentra forjada por una comunidad ética y política destinada a alcanzar la vida buena bajo los principios de la justicia y la virtud, por ello implícitamente requiere protección de aquellos que buscan destruirla. Esto quiere decir que es necesario protegerse contra el enemigo desde dos posturas: aquellos que provienen del exterior y los que pueden surgir del seno mismo de la polis.

El enemigo externo es aquel que representa una amenaza física y política que proviene desde fuera de la propia polis; el cual, puede ser otro Estado o cualquier otra fuerza que pretenda destruir la seguridad de una comunidad política. Desde la óptica de Aristóteles, la defensa contra este enemigo sería legítima y hasta necesaria; en la medida en que resguardaría la supervivencia de la polis.

Por lo tanto, la posibilidad de que los ciudadanos vivan efectivamente su vida política bajo la justicia y la virtud, implica que la guerra contra el enemigo externo se configure como un medio idóneo para proteger el orden interno y el mantenimiento del orden pacífico.

En cambio, el enemigo interno es más sutil, Aristóteles considera que dentro de la polis puede haber individuos o grupos que actúan en contra del bien común y de la justicia, poniendo en peligro tanto la estabilidad política como la estabilidad mora.

Esto son denominados enemigos internos como: los tiranos, los subversivos del orden legal o tenemos aquellos que defienden conductas injustas que pueden hacer estallar la comunidad política; pero, su trato debe encontrarse sobre el principio de justicia y sobre el respeto por la ley.

De allí, que la legitimidad del Estado precisamente se encuentra en su capacidad de administrar justicia y evitar las arbitrariedades que destruyen la cohesión social, si bien con un trato diferencia del enemigo pero matizado en la ley del Estado y su legitimidad para conseguir el bienestar común.

No obstante, no fue el único que se refiere a esta figura, Marlene Román citada por Kai Ambos (2007) señala que en el derecho romano, establecía una distinción entre el *inimicus* y el *hostis:* El primero era el enemigo particular, mientras que el segundo representaba al enemigo político, el cual siempre resulta susceptible de guerra. El hostis sería entonces la negación más absoluta del otro o la mayor intensidad de la hostilidad y, por ende, el enemigo de todos o el enemigo político.

Marco Tulio Cicerón, filósofo y jurista de la antigua roma, reflexiona sobre esta figura continuando con la tradición de diferencia entre enemigo externo e interno, en cuanto al primero, se origina fuera del cuerpo político romano sometido a la protección del ius gentium.

El mismo establece, que la guerra que se hace contra otros debe ser justa, es decir, ha de llevarse a cabo por causa de exigencias legítimas y declarada por la persona que posea la autoridad suficiente para ello en aras de perseguir la paz. Incluso, en el conflicto bélico Cicerón abriga la defensa de ciertos límites jurídicos/morales y acepta como necesario establecer que el enemigo exterior—el rival—es un sujeto de derecho.

El enemigo interior, por el contrario, es el más peligroso para la República, pues es un ciudadano que coacciona el orden jurídico y moral desde el interior. Este enemigo (como el tirano), no se encuentra sometido al derecho de gentes, sino que se transforma en un *hostis publicus*; figura que implica su exclusión total del orden jurídico y político.

Lo expuesto, en virtud de haber quebrantado el pacto cívico, por lo que su eliminación puede considerarse legítima y sin que medie juicio. El tirano es la forma más grave del enemigo interior, que es quien desde el poder arrasa la legalidad de la república.

Ahora bien, el Digesto parte del Corpus Iuris Civilis, también distingue entre enemigos externos e internos:

> (...)enemigos son aquellos con los que entramos en guerra, en general, ladrones y piratas. También es enemigo aquel que, con mala intención y espíritu traicionero, abandona la patria; pero no lo es, sin embargo aquel con quien existe una relación de amistad, hospitalidad o análogas.(Ambos**,** 2007, p. 10, 11)

No obstante, para Marlene Román (2009) el concepto del "enemigo" fue concebido de manera anterior al derecho, desde el contractualismo filosófico, una de sus más grandes figuras fue el tan referido Thomas Hobbes, que como se observó en un capítulo anterior, bajo el Leviatán, el enemigo es quien vulnera el acuerdo y amenaza la seguridad de los pactantes y puede ser aniquilado sin miramientos ya que el enemigo es, en suma, el retorno a lo natural.

En contraposición para John Locke, el enemigo es, en consecuencia, aquel que actúa en contra de la ley natural, el hombre ha dejado de usar la razón y busca quebrantar el pacto civil, comparándolo incluso con una bestia salvaje león o un tigre, el cual no puede ser persuadido ni juzgado, sino que ha de ser repelido y destruido en legítima defensa.

El enemigo no es, pues, solamente perpetrador de un delito, sino que es alguien que se niega a aceptar el principio de la convivencia racional y pacífica.

Frente a esa amenaza, Locke afirma que el individuo tiene el derecho natural a resistir a la agresión; también tiene lugar dentro del ámbito político, de manera tal que si el gobernante traiciona el pacto social y ejerce un poder arbitrario que va en contra de los intereses del pueblo, entonces los ciudadanos poseen no solo el derecho, sino también la obligación de ejercer dicha resistencia.

En ese contexto, el tirano queda convertido en enemigo del pueblo y por ende ya no hace uso de su poder legítimo, sino que hace uso del poder por medio de la fuerza.

Para Rousseau, el ser humano es libre e inocente en el estado de naturaleza, la corrupción de la persona viene con la propiedad privada y la sociedad desigual. En cambio, el verdadero

contrato social es el que da lugar a la voluntad colectiva, manifestación del poder soberano del pueblo; de esta manera, el enemigo de la comunidad política no es solo quien comete el delito sino aquel que actúa contra la voluntad general y pone en peligro la unidad del cuerpo del cuerpo colectivo.

En efecto, Jean-Jacques Rousseau al establecer dentro de su obra que "cualquier delincuente o malhechor que ataque el "Derecho Social" deja de ser "miembro" del Estado; en estos casos, la pena contra ese malhechor supone que se halla en guerra contra el Estado" (Gómez & Cifuentes, 2011 p.11).

A ojos de Rousseau, quien traiciona la soberanía dejará de ser ciudadano y se convertirá en enemigo, por lo que puede ser expulsado o castigado por el conjunto soberano, constituyendo así el enemigo aquel que niega el pacto al romper la unidad del pueblo.

De manera paralela, Johann Gottlieb Fichte sostenía que aquel ciudadano que abandone el contrato social en el que este es requerido "sea de modo voluntario o por imprevisión, en sentido estricto pierde todos sus derechos como ciudadano y como ser humano y pasa a un estado de ausencia completa de derechos" (Gómez & Cifuentes, 2011 p.11.).

Por otra parte, otros autores como Guillermo Portilla y Eugenio Zaffaroni (2011a) sitúan sus antecedentes en la teoría política de Carl Schmitt, quien distingue entre amigos y enemigos, de la siguiente manera:

> Enemigo no es pues cualquier competidor o adversario, tampoco es el adversario privado al que se detesta por cuestión de sentimientos o antipatía, el enemigo es sólo un conjunto de hombres que siquiera eventualmente, esto es, de acuerdo con una posibilidad real, se opone combativamente a otro conjunto análogo. Solo es enemigo, el enemigo público, pues todo cuanto hace referencia a un conjunto total de personas, o en términos más precisos a un pueblo entero (Delgado, 2011, p.4).

Frente a los postulados de los filósofos contractualistas Rousseau y Fichte quienes buscaban una marginalización total del criminal por parte del Estado, el jurista Jakobs en su teoría

discrepó de sus aportes por su generalidad, para el alemán un sistema legal debe incluir al criminal por dos motivos fundamentales:

El infractor conserva el derecho a reinsertarse en la sociedad y, a su vez, tiene la obligación de resarcir el daño derivado de su conducta delictiva, por lo tanto, no puede desvincularse arbitrariamente de la sociedad a través de su acto criminal (Gómez & Cifuentes, 2011).

En cuanto a la Teoría de Carl Schmitt, Jakobs niega explícitamente esta relación, pero académicos como Guillermo Portilla Contreras, Eugenio Zaffaroni, Francisco Muñoz Conde, Kai Ambos, Eduardo Demetrio Crespo o Bernd Mussig, señalan la conexión entre el enemigo de Jakobs y el concepto de Schmitt.

2.2.3 La delimitación del concepto de persona en el Derecho Penal de Günther Jakobs: entre el ciudadano y el enemigo

La postura del enemigo, surge frente a amenazas que ponen en jaque el orden social y activa la necesidad del Estado de auto preservarse frente a quienes niegan las condiciones básicas de convivencia.

De allí que, el profesor alemán Gunter Jakobs desde mediados de los años ochenta, en una conferencia denominada *Criminalización en el estadio previo a la lesión de un bien jurídico* de 1985 en Frankfurt introdujera este concepto; con el objetivo, de generar una respuesta frente al aumento de delincuencia provocada por una profunda crisis de seguridad que afectaba la República Federal de Alemania para esos momentos; pero fue hasta 1999 que comenzó a tener eco en la comunidad jurídica frente a delitos graves.

El Derecho Penal desde una mirada funcionalista y sistémica, fuertemente condicionado por la teoría de sistemas de Niklas Luhmann, es un mecanismo de control social al servicio de la estabilidad del orden jurídico.

Sobre esta base teórica Jakobs edifica una de sus propuestas más discutidas: el Derecho Penal del Enemigo, teoría que, aunque en primera instancia elaborada, en principio como una advertencia crítica, acaba por adquirir un perfil estructural en su obra constituyendo un modelo que presenta la opción de excluir jurídicamente a ciertos sujetos considerados como amenazas sistemáticas para el orden social.

La teoría jurídica de Gunter Jakobs, como se ha manifestado parte de identificar en el ordenamiento jurídico penal dos destinatarios: el ciudadano (Bürgerstrafrecht) y el enemigo (Feindstrafrecht), cada sujeto amparado bajo un sistema jurídico diferente, cimentado en si la norma lo reconoce o no como persona. Es bajo la concepción de persona que el jurista estructura su funcionalismo sistémico.

Apartado del enfoque tradicional del iusnaturalismo para Jakobs el ser humano no equivale a ser persona; pues el primero alude a una realidad ontológica incluso en su sentido biológico, mientras que persona es una creación del derecho, Jakobs (1996) establece que "una sociedad existe cuando está vigente al menos una norma. Y por norma debe entenderse la expectativa de que una persona, en una situación determinada, se comportará de una manera específica, solo y exclusivamente debido a su ser persona" (p. 17).

Así, establece que se es persona por la construcción normativa que surge del propio entramado social; la persona se materializa dentro del rol que ocupa el individuo, esto es comportarse desde la previsibilidad de la norma o conforme a ella.

Retomando esta diferencia, Daniel Alonso Almeyda Velásquez (2015) establece que para "Jakobs, persona en Derecho significa tener que representar un papel, es la representación de una competencia socialmente comprensible, dicho en otras palabras, quien es portador de un rol en sociedad (sujeto mediado por lo social)" (p. 97).

Con esto en mente, el subsistema de derecho no protege la condición de ser humano, sino la capacidad de que este cumpla roles fijados por la ley. Jakobs (2004)señala que "la persona jurídica se constituye como tal en el momento en que es reconocida como participante del

intercambio comunicativo del Derecho" (p. 47); es decir, esta categoría se trata de una ficción funcional que posibilita la comunicación normativa.

De este modo, se perfila la columna vertebral de la teoría funcionalista; y es que el ser humano no vale por su condición intrínseca, sino en medida que garantiza la vigencia de la norma social; en opinión de los autores Torres Vásquez, Tirado Acero y Trujillo Florián (2018) "el Funcionalismo considera que la dignidad es únicamente atribuible a quienes por causa de su comportamiento y amistad con el Estado y su seguridad la han ganado" (p.186).

Una percepción utilitarista de la figura en la medida que no formula un juicio moral sobre el valor que presenta el ser humano, sino el estatus de la persona como rol funcional en el sistema otorgado por el mérito y desempeño del mismo. El individuo no es parte central del derecho sino un pieza del engranaje social, cuyo reconocimiento está supeditado a su utilidad comunicativa; cuanto más estable su comportamiento, mayor su reconocimiento como persona en el sistema.

Si se traslada este esquema al terreno de la utilidad social, el reconocimiento del ser humano como persona-sujeto de derechos y obligaciones- "no es fijada de manera arbitraria o deliberada, sino con el deseo o más precisamente con la aptitud de aquél de aceptar organizarse adecuadamente en sociedad, mejor dicho, debe cooperar" (Almeyda, 2015,p.98), en sí la cooperación está dada cuando el ser humano construye su identidad conforme a los parámetros de una sociedad o en relación con los demás.

De allí que, un nuevo componente se presenta: el individuo útil es previsible en lo jurídico y también (producto) en lo social. Su valor (útil) se constituye a partir de su capacidad de mantener el flujo de comunicación y la cooperación social, cuando este no coopera y decide autoexcluirse del sistema deja de ofrecer una base confiable de comunicación normativa.

En palabras de Jakobs (2004), "quien no ofrece garantías cognitivas mínimas de comportamiento conforme, deja de ser persona en Derecho" (p. 49). Este mínimo confianza cognitiva (*kognitive Sicherheit*) se determina no por un elemento subjetivo o psicológico, sino por medio de un requisito funcional y es que la sociabilidad se basa en expectativas recíprocas de

comportamiento; en otras palabras, cada miembro del sistema confía en que los demás actuarán conforme a derecho.

Todo individuo debe ser previsible y cooperativo, de modo que su comportamiento permita a los demás orientarse y confiar en la continuidad del orden social. Si cada individuo estableciera un mundo propio con pretensión de generalidad, como advierte el propio Jakobs, se regresaría a un estado de naturaleza regido por el binomio apetencia/inapetencia, satisfacción/insatisfacción, es decir, por el interés individual y no por la norma (Almeyda, 2015).

La persona, en esta perspectiva, no es un fin en sí misma, sino un medio para la preservación de la confianza en el sistema normativo, pues debe cooperar e integrarse al proceso comunicativo del sistema jurídico y prestar lo que Jakobs denomina un "apoyo cognitivo" a los demás miembros de la comunidad, al servir como punto de orientación para los otros en su comportamiento. Dicho de otro modo, debe comportarse de manera que los demás puedan orientar sus expectativas tomando como referencia su conducta.

En consecuencia, si el sujeto decide crear sus propias reglas o responsabilidades y derechos enfrentados a los socialmente vigentes, será alguien a quien los demás no pueden confiar y no pueden establecer esta base cognitiva necesaria para poder orientarse en la vida social.

Lo anterior, es una concepción hobbesiana del asunto de referencia pues permite establecer que es la norma la que hace sociable al hombre; ya que al generar un comportamiento contrario a derecho, la confianza colectiva se pierde, el sistema puede colapsar y se sustituye por la fuerza. Un quebrantamiento claro del pacto social.

Ahora bien, esta concepción funcional de la persona tiene consecuencias directas en el modo en que Jakobs entiende la estructura del Derecho Penal; en verbigracia, si el estatus de persona depende de la cooperación normativa y de la fiabilidad de la conducta, el Derecho no puede trazar la disección de manera equivalente en aquellos que confirman el orden jurídico y en quienes lo niegan radicalmente.

Lo desarrollado previamente, permite inferir que el tratamiento penal que se le da a los individuos que conforman el sistema, dependerá de manera indisoluble a la relación que estos mantengan con la norma.

Por lo tanto, la forma en que una persona se vincula al Derecho (cooperando o negando la norma) determina la forma en que el sistema penal actuará, pues para Jakobs “lo que está en juego no es la protección de bienes legales, sino más bien la garantía de la validez de la norma” (Pereira, Souza & Cimolin, 2021, p. 37)

De esta manera, el Derecho Penal del ciudadano, es una categoría de aplicación clásica y tradicional donde el que infringe la norma sigue siendo tratado como persona, lo cual, parte de la idea de que el sujeto pese a haber defraudado la expectativa normativa, no ha quebrantado el pacto social o abandonado las reglas mínimas de convivencia, por lo que solo basta la pena para reafirmar la norma frente a la sociedad.

Tabla 7

Derecho Penal del ciudadano vs Derecho Penal del enemigo.

Característica	Derecho penal del ciudadano	Derecho penal del enemigo
Objetivo	Mantiene la vigencia de la norma y el orden social	Aumenta la punibilidad y neutraliza el peligro
Derechos del imputado	Asegura el respeto de los derechos y las garantías procesales	Puede implicar la suspensión de ciertos derechos
Función de la sanción	Restaurar el equilibrio social y permitir la reintegración	Prevenir peligros futuros más que castigar acciones pasadas
Estatus del infractor	Reconocido como persona y titular de derechos	Deja de ser considerado plenamente como persona

Fuente: Elaboración propia en Napkin con base en (Almeyda, 2015)

En principio, el Derecho Penal cumple la función de mantener el orden social y los intereses colectivos que se desprenden él, si bien existe un abandono del rol por parte del individuo, este puede ser reconducido a la normalidad mediante la imposición de una pena, que a su vez reafirma que el orden jurídico continúa vigente, pues su comportamiento aún permite la comunicación. "Quien infringe la norma, pero no la niega, sigue siendo miembro de la sociedad jurídica, pues con su sanción confirma la vigencia de la regla que ha transgredido" (Jakobs, 2003, p. 38).

Razón por la cual, el ciudadano, en la teoría de Jakobs, se articula sobre la premisa de que la persona, aun cuando delinque, no cuestiona la totalidad del orden jurídico, sino que transgrede una parte de él; por ende, se identifica como una persona a quien se le reconoce dignidad jurídica, titular de derechos fundamentales y sujeto de garantías procesales.

El Derecho Penal del ciudadano, el sujeto sigue siendo un interlocutor, es capaz de entender de manera clara la sanción impuesta por su conducta desviada y tiene intención de recuperar su rol en la sociedad es decir reinsertarse al orden normativo previsto.

Así pues, el Derecho Penal comprende tres posturas convergentes: sanciona al infractor, mediante la sanción reafirma los lazos jurídicos que los vinculan con el orden social y es una reacción del ius puniendi para restaurar la confianza en la expectativa normativa quebrantada.

Como manifiesta el jurista Pablo Elías González Monguí (2019) al citar a Jakobs:

> El ciudadano es una persona que mediante su conducta ha dañado la vigencia de la norma y que por ello es llamado, de modo coactivo (mediante la pena), a equilibrar el daño con el restablecimiento de la vigencia de la norma (Jakobs, 2003) y ofrece garantía de actuar con fidelidad al ordenamiento jurídico (p. 1074).

A la luz de este derecho, se observa la aplicación de un Derecho Penal clásico desde un ámbito funcional donde el Derecho Penal opera dentro de los límites de comunicación y garantías fundamentales al desarrollarlo dentro del marco de un instrumento de equilibrio social.

Sin embargo, este esquema se sostiene solo mientras el infractor continúe prestando un mínimo de apoyo cognitivo al sistema. Cuando el sujeto rompe completamente la posibilidad de comunicación —cuando su conducta niega el orden jurídico en su totalidad y se vuelve impredecible—, el Derecho Penal del ciudadano deja de serlo.

En ese momento, la pena ya no puede cumplir su función simbólica y el Estado comenzara a transitar hacia otra lógica que no es la de la comunicación, sino la de neutralización del peligro: es ahí donde empieza a configurarse el Derecho Penal del Enemigo (DPE), orientado no a la comunicación, sino a la defensa.

2.2.4. Fundamentos, alcances y crítica al Derecho Penal del enemigo en Günther Jakobs.

Continuando con este razonamiento, la conceptualización de qué se entiende por enemigo es una categoría analítica y descriptiva de la teoría, Jakobs no busca crear un enemigo y sustentar sus características, lo que busca es detallar un fenómeno que ya ocurre dentro de los sistemas penales contemporáneos (Almeyda, 2015). En efecto, el profesor Günter aclara:

> (…)no es mi propósito convertir a alguien artificialmente en enemigo, sino describir a quien el sistema jurídico trata como enemigo y pronosticar a quién atribuye en el futuro ese papel. No se trata de crear normas, ni mucho menos de formular postulados políticos, sino de llevar a cabo constataciones y de sus prolongaciones. (Jakobs G, 2007b, p. 21).

Tal direccionamiento marca una pauta: su teoría no busca justificar un régimen autoritario bajo marcos normativos de excepcionalidad, es visibilizar que en ordenamientos clásicos actuales fundados en garantías constitucionales contienen prácticas propias que enmarcan una figura de enemigo.

Jakobs no busca impulsar a Estados a actuar de esta manera, sino constatar que lo hacen bajo el marco de la priorización de seguridad pública.

Sus reflexiones teóricas, sobre el tratamiento penal que se debe dar a aquellos individuos considerados como enemigos del orden social, se basa en la premisa de que existen personas que

representan una amenaza constante para la sociedad y que deben ser tratadas de manera diferente a los delincuentes comunes, por ello su teoría se dirige precisamente a aquellos sujetos calificados como enemigos o "no personas" al interior de los Estados.

La noción del enemigo surge, entonces, de la ausencia de un mínimo confianza cognitiva; el enemigo no es definido por su maldad moral, sino por su incapacidad o negativa de cooperar con el sistema normativo.

Para Jakobs el enemigo deja de ser interlocutor del derecho, demostrando que en su comportamiento encarna (modo de vida, profesión, participación en organizaciones criminales) un rechazo continuo a las normas que forjan el pacto social.

En consideración, Natalia Andrea Bravo (2007) dispone que existe el enemigo cuando infringe de manera consciente y prolongada la norma sin que excita en el individuo una retractación de la misma o de volver a actuar en su rol.

En consecuencia, el proceso para que una persona se desplace a enemigo está dada a partir de "la reincidencia, la habitualidad, la profesionalidad delictiva, pero en sobremanera por pertenecer a organizaciones que se enfrentan al derecho y ejercer cualquier tipo de actividad que lo vinculen a ellas" (p.82)

De este modo, la representación del enemigo no es otra que la del individuo que ha renunciado por voluntad expresa y organizada al contrato social; habida cuenta de que no solo infringe las normas, sino que hace desaparecer la validez del sistema jurídico-político en su totalidad.

De acuerdo con Luis Martin Gracia (2005)

> (...) los enemigos son individuos que se caracterizan primero, porque rechazan por principio la legitimidad del ordenamiento jurídico y persiguen la destrucción de ese orden y, segundo, a consecuencia de ello, por su especial peligrosidad para el orden jurídico, dado

> que tales individuos no ofrecen garantías de la mínima seguridad cognitiva de un comportamiento personal, es decir, su comportamiento ya no es calculable conforme a las expectativas normativas vigentes en la sociedad (p.7).

Para Jakobs, estos sujetos no pueden ser tratados como ciudadanos comunes ya que representan una amenaza activa y permanente contra el orden jurídico; de tal manera que pierden la condición de persona jurídica plena, y pasan a ser considerados fuentes de peligro que deben ser neutralizadas; distanciándose del tratamiento penal tradicional, adentrándose a la espera de lo preventivo de la anticipación punitiva.

El enemigo ya no se considera plenamente persona. El enemigo es, jurídicamente, una cosa y no un sujeto de derecho; la dignidad humana, que hace de frontera infranqueable en la idea del Derecho Penal del Ciudadano, es sustituida por el principio de seguridad.

Cabe resaltar que la categoría de enemigo se sustenta en tres principios: El primero es que no todos los individuos son iguales ante la ley; en segundo lugar, el ser humano no es un ser humano, es una persona y el tercero, considera que una persona puede ser persona o no persona (Parma, 2009).

De esta forma, el enemigo se autoexcluye de la comunidad jurídica; no es el Estado quien lo expulsa, es él mismo quien se coloca fuera del marco normativo.

Por tanto, no puede exigir el mismo trato juicio de quienes sí se someten a las reglas, de allí que sea retirado del ordenamiento jurídico heteronormativo y se genere un tratamiento excepcional para hacerle frente. "Tratándose del enemigo, como no presta seguridad cognitiva- dice Jakobs-, no se debe recibir el mismo trato que se le dispensa al ciudadano, porque aquél vulnera el derecho a la seguridad de los considerados como personas" (González Monguí, 2019, p. 1089).

Jakobs, como se ha mencionado, retoma la noción hobbesiana del estado de naturaleza, el individuo retorna a este estado primitivo, donde el Estado puede ejercer su poder no como

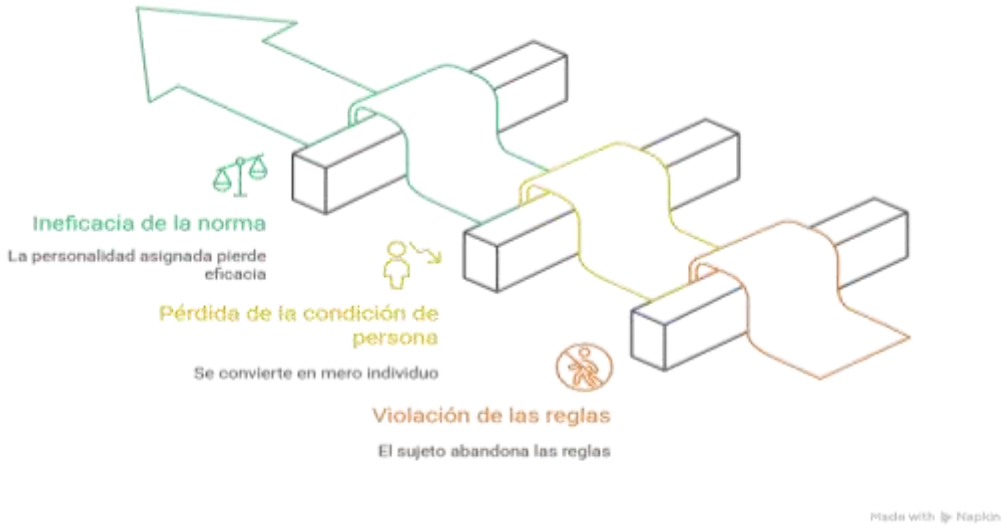
autoridad jurídica, sino como fuerza de contención o eliminación. Como resultado, genera una función simbólica de identidad de lo que el sistema jurídico no es y los valores que sostiene.

Ahora, la figura del enemigo no obedece o posee rasgos característicos más que ser una amenaza considerable para el sistema, razón por la que es una figura contingente que depende del contexto histórico y social de la época; convirtiéndose en un instrumento de situaciones excepcionales que justifican un tratamiento penal diferenciado en defensa de la seguridad y la cohesión del sistema social.

Con todo, ante la eventual falta de confianza recíproca entre el sistema y el individuo, el Derecho Penal del ciudadano deja de ser efectivo, porque su diseño se enfoca en aquellos que continúan reconociendo al ordenamiento jurídico, no aquel que combate abiertamente el propio sistema; para estos individuos Jakobs crea un sistema jurídico penal diferenciado y excepcional que opera con base en la neutralización del peligro que representa el enemigo.

Figura 17.

La pérdida de personalidad según Jakobs.



Fuente: Elaboración propia en Napkin con base en (García Amado, 2006)

Jakobs propone diferentes niveles para solucionar la disfuncionalidad social, desde la infracción común o delincuencia ordinaria a la negación sistemática del orden social, según el jurista Pablo Elías González Monguí (2019):

> Para efecto de esa coacción, el Estado puede proceder de dos modos con los delincuentes: con respecto a los ciudadanos, con coacción mediante la pena, pero logrando el restablecimiento de la vigencia de la norma. Con respecto al enemigo, es sólo coacción física y combate de peligros hasta llegar a la guerra (p. 1075).

La Teoría del Derecho Penal del Enemigo, en adelante TDPE, "es el conjunto de normas excepcionales que se dirige a individuos que se han apartado de forma duradera del derecho, es decir, que no reconocen la vinculación del sistema jurídico"(Almeyda, 2015, p. 111).

Con este derecho no se busca mantener la vigencia de la norma, pues no existe expectativa a mantener (el individuo ya no forma parte del sistema), se pretende neutralizar un peligro futuro de quien ha decidido no cumplir su rol.

El TDPE, busca el restablecimiento del mínimo de confianza cognitiva; luego, no es un ordenamiento de comunicación normativa sino un instrumento de aseguramiento que no reprocha las conductas punibles del pasado sino las futuras amenazas, es decir una función meramente instrumental de seguridad para evitar que el enemigo cause un daño irreparable al pacto social; "lo que se busca es la neutralización del peligro futuro de quien ha decidido no vivir en sociedad" (Jakobs G, 2003, p. 49).

La esencia de la TDPE, se encuentra en su carácter preventivo y peligrosista; en otras palabra, no actúa bajo el enfoque de la retribución clásica, sino por la necesidad de garantizar condiciones previsibles de convivencia, buscando restaurar un equilibrio no mediante la comunicación sino la neutralización.

El concepto de neutralización o neutralizar resulta clave para comprender esta teoría; según la Real Academia Española (RAE, 2024) el término significa: "Contrarrestar el efecto de

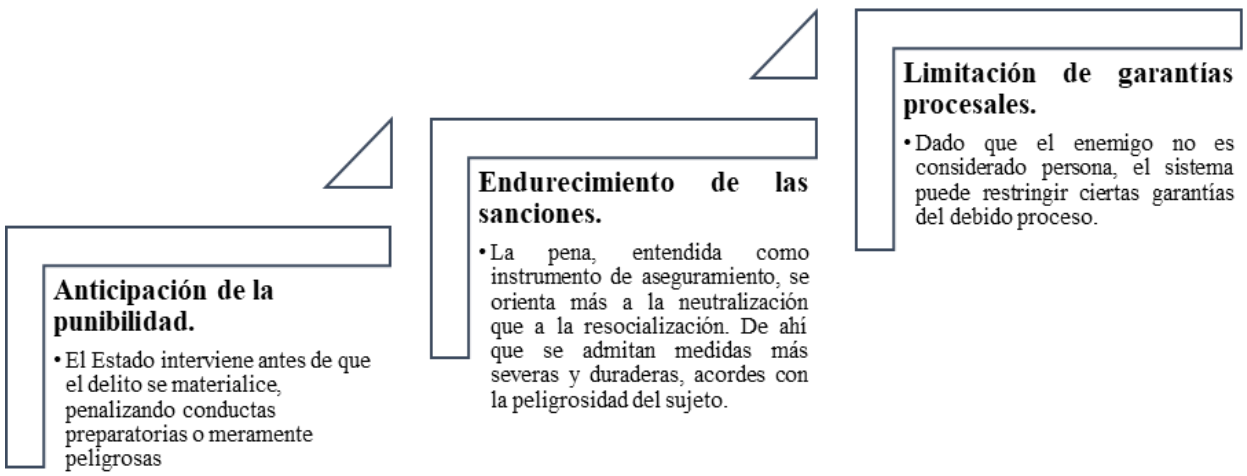
una causa por la concurrencia de otra diferente u opuesta" o "Anular, controlar o disminuir la efectividad de algo o de alguien considerados peligrosos".

Las anteriores definiciones reafirman que frente a la TDPE, se busca a través de la prevención contener o incluso anular el peligro representar por quienes han dejado de ofrecer confianza mínima en el cumplimiento del ordenamiento; en virtud de ello, la neutralización implica preservar la seguridad a partir de la coacción.

Ante el evento de hacerse operativo y teniendo en cuenta que la categoría de persona se encuentra aislada, la TDPE posee tres consecuencias inevitables de su lógica funcional:

Figura 18.

Consecuencia de la implementación del TDPE.



Fuente: Elaboración propia con base en (Sánchez, 2009)

Estas características, lejos de convertirse en una adopción de regímenes autoritarios, es un representación conceptual de cómo el Derecho Penal actúa cuando su función principal de comunicación fracasa y solo queda su forma primitiva, una realidad jurídica límite en que el Estado

actúa por supervivencia, donde el derecho actúa en su defensa; es decir, una forma de resistir ante la anomia.

El Estado, para compensar ese déficit de apoyo cognitivo que presenta la figura del enemigo debe dirigirse a la coacción, pues de garantizar una libertad completa al individuo que no cumple un rol social, puede convertirse en un riesgo para la permanencia de la comunidad misma, por ello la TDPE no busca destruir al enemigo, busca administrar el uso defectuoso de su libertad, desde su despersonalización como no persona (Almeyda, 2015).

Su despersonalización es parcial, si bien se restringen garantías del debido proceso al individuo, el enemigo no pierde toda su calidad persona, solo en el ámbito jurídico penal relacionado con su peligrosidad, como explica el profesor alemán:

> El ámbito de lo personal retrocede a un segundo plano y el ámbito del enemigo se adelanta al primer plano cuando a la persona se le recortan sus derechos porque, al menos parcialmente, no se espera de ella una conducta futura adecuada a Derecho (Jakobs G, 2003, p. 37).

Con ello, Jakobs, es claro en distinguir este derecho como último recurso del Derecho Penal, por cuanto el Derecho Penal enemigo está actuando más allá de la construcción del contrato social, es su manifestación más extrema: la función de aseguramiento del orden jurídico.

En palabras de Miguel Polaino-Orts (2012), este Derecho "es la última ratio de la última ratio que es el Derecho Penal"(p.36).

Razón por la cual, para Jakobs, es indispensable diferenciar claramente entre los receptores del Derecho Penal: enemigo y ciudadano. En un Estado de Derecho sería inadmisible el trato de un enemigo como ciudadano, o viceversa, para el caso sería deshonesto por cuanto el derecho negaría su autoexclusión del orden jurídico.

Cabe destacar que se debe ser claro que para generar esa diferenciación se encuentra en el grado de previsibilidad de conducta futura: cuanto menor sea la expectativa de actuar conforme al Derecho, mayor será la aplicación del TDPE.

La TDPE debe aplicarse de modo excepcional y restrictivo, para evitar que la lógica de la seguridad desplacé a la de la juridicidad, así lo estima pertinente el jurista alemán cuando dispone que es "tarea aún recién iniciada de la ciencia la de identificar las reglas del Derecho Penal del Enemigo y separarlas del Derecho Penal del ciudadano para, dentro de este último, insistir con mayor firmeza en el tratamiento del delincuente como persona" (Jakobs G, 2003, p. 47).

La TDPE se justifica como mecanismo de contención cuyo objetivo es limitar no sólo la amenaza que significa la existencia de ciertas personalidades criminales en la sociedad; de igual manera, recordar cuáles son los riesgos que administra el Estado de Derecho bien entendido al extender sin medida la TDPE

Bajo este referente, derivado del desarrollo de este capítulo, se presentan los fundamentos que sustentan la creación de la TDPE elaborada por Günther Jakobs, de la siguiente manera:

En primer lugar, se encuentra la *dicotomía entre ciudadano y enemigo*, que hace referencia precisamente en el desarrollo de dos sistemas punitivos contarios, sustentado en el trato desigual que deriva en sus destinatarios: por su parte el ciudadano "persona" que reconoce la validez del orden social, aunque cometa delitos; y el enemigo "no persona" que niega ese orden de manera sistema y persistente, considerado una amenaza a neutralizar.

En segundo lugar, Jakobs parte del *funcionalismo sistemático* inspirado en Niklas Luhmann, bajo este precepto se erige la función del Derecho Penal como instrumento de estabilización de expectativas normativas donde se prevé la prevalencia del orden social sobre la protección de derechos individuales.

En tercer lugar, se vislumbra el *Derecho Penal del autor,* este enfoque implica que la persona es penalizada no por su actuar, sino por quien es. Lo anterior, por cuanto existe un

desplazamiento hacia la prevención castigando a sujetos con conductas o perfiles considerados amenazantes, incluso antes de efectuar algún actuar delictivo.

En cuarto lugar, proveniente de este carácter peligrosista se desarrolla *la anticipación de la punibilidad*, esto se traduce a sancionar conductas en fases muy tempranas, por la potencialidad del riesgo frente al pacto social, llegando a sancionar etapas preparatoria o de simple sospecha.

En quinto lugar, se sopesa la *reducción de garantías procesales*, pues el enemigo al no ser persona dentro del Derecho Penal, no puede ser juzgado bajo las misma condiciones que el ciudadano común, por lo que se reducen o restringen derecho fundamentales como la presunción de inocencia, el debido proceso y la libertad personal, entre otras garantías.

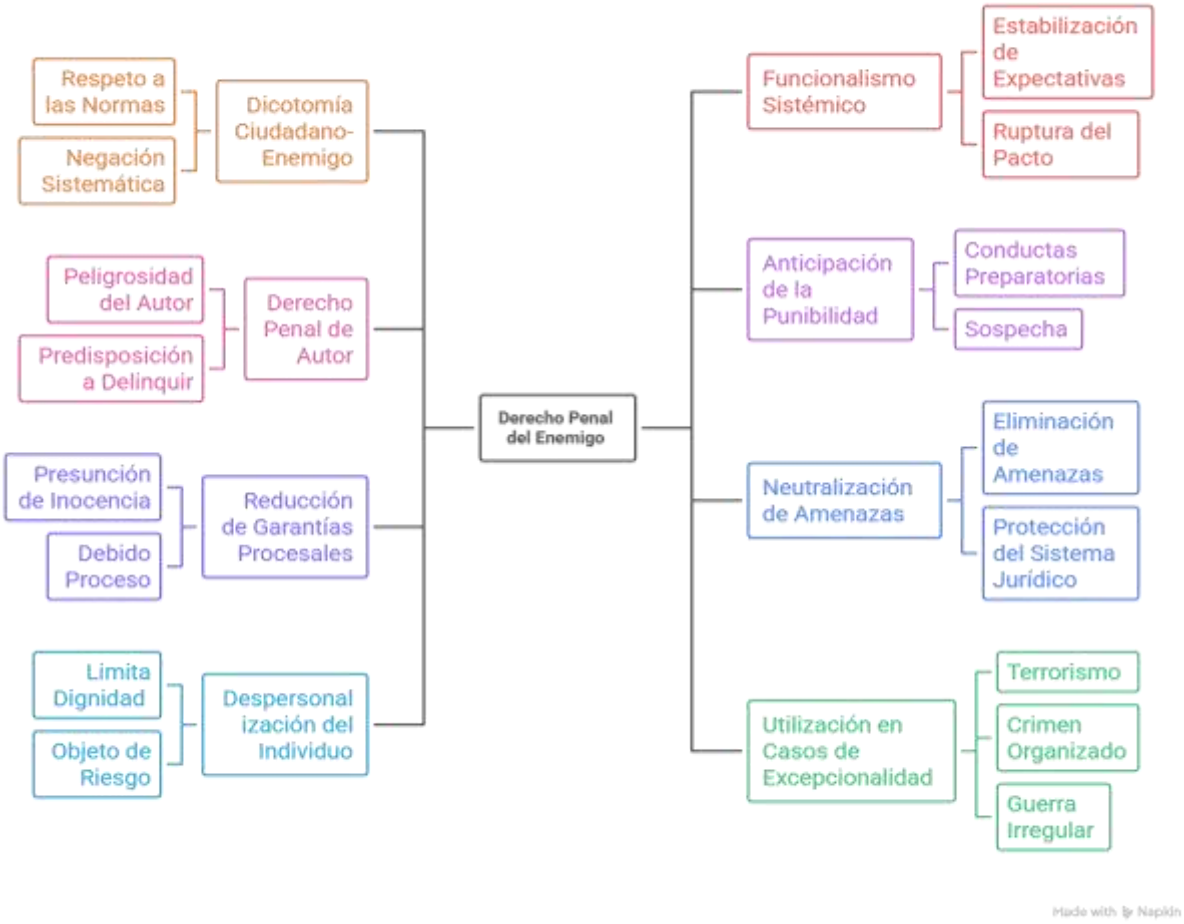
En sexto lugar, el objetivo de la TDPE no es la reinserción, si no la *neutralización de amenazas*; considerando que el enemigo puede destruir el pato social, este debe ser contenido o eliminado en su defecto antes de que logre actuar.

En séptimo lugar, la *despersonalización del individuo*, que deriva de la categoría de "no persona" determinada por la norma genera una pérdida de la dignidad humana del individuo y pasa a ser tratado como un objeto de riesgo.

Por último, su *aplicación excepcional* concurre con contextos históricos donde se activa para hacer frente a amenazas extraordinarias que el propio ordenamiento identifica.

Figura 19.

Fundamentos Teóricos del TDPE.



Fuente: Elaboración propia.

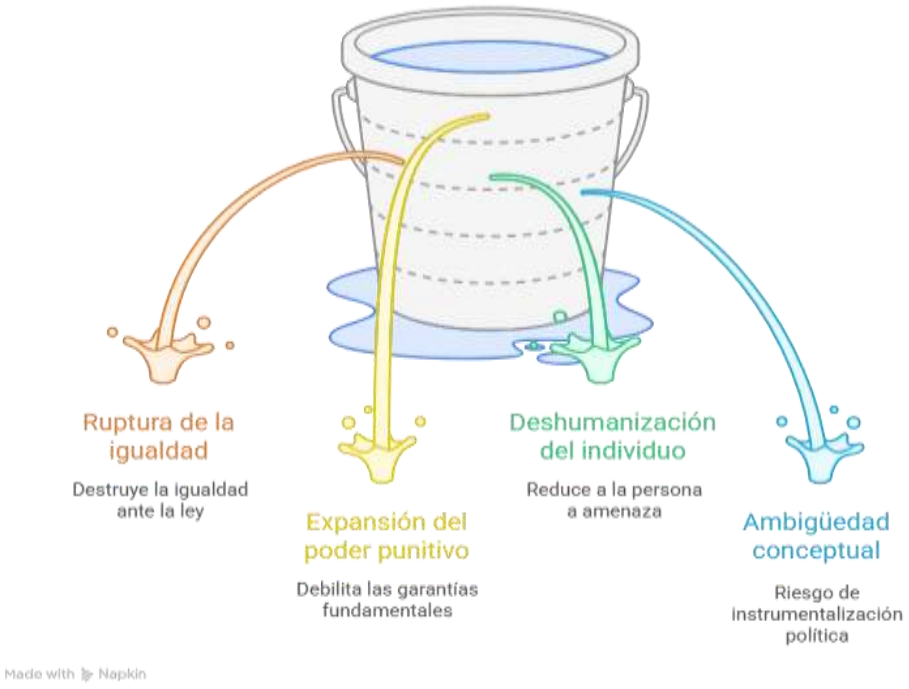
De este modo, el TDPE se configura como método jurídico de defensa preventiva, que, si bien puede parecer comprensible frente a amenazas de gran magnitud, implica un giro radical: pasa de un modelo centrado en la persona y sus derechos, a otro enfocado en la preservación funcional del sistema frente al peligro que representan ciertos individuos.

La TDPE ha suscitado una amplia gama de críticas y debates en la doctrina penal contemporánea debido a sus profundas implicaciones teóricas y éticas.

Este modelo funcionalista con base en los fundamentos teóricos narrados, trasciende las líneas propias de la moral al distinguir entre el ciudadano —como sujeto de derechos— y el enemigo —como amenaza a la estabilidad del Estado— lo cual plantea tensiones en torno a la vigencia de los principios fundamentales del Estado de Derecho, como frente a los derechos humanos.

Figura 20.

Críticas a la Teoría de Gunter Jakobs

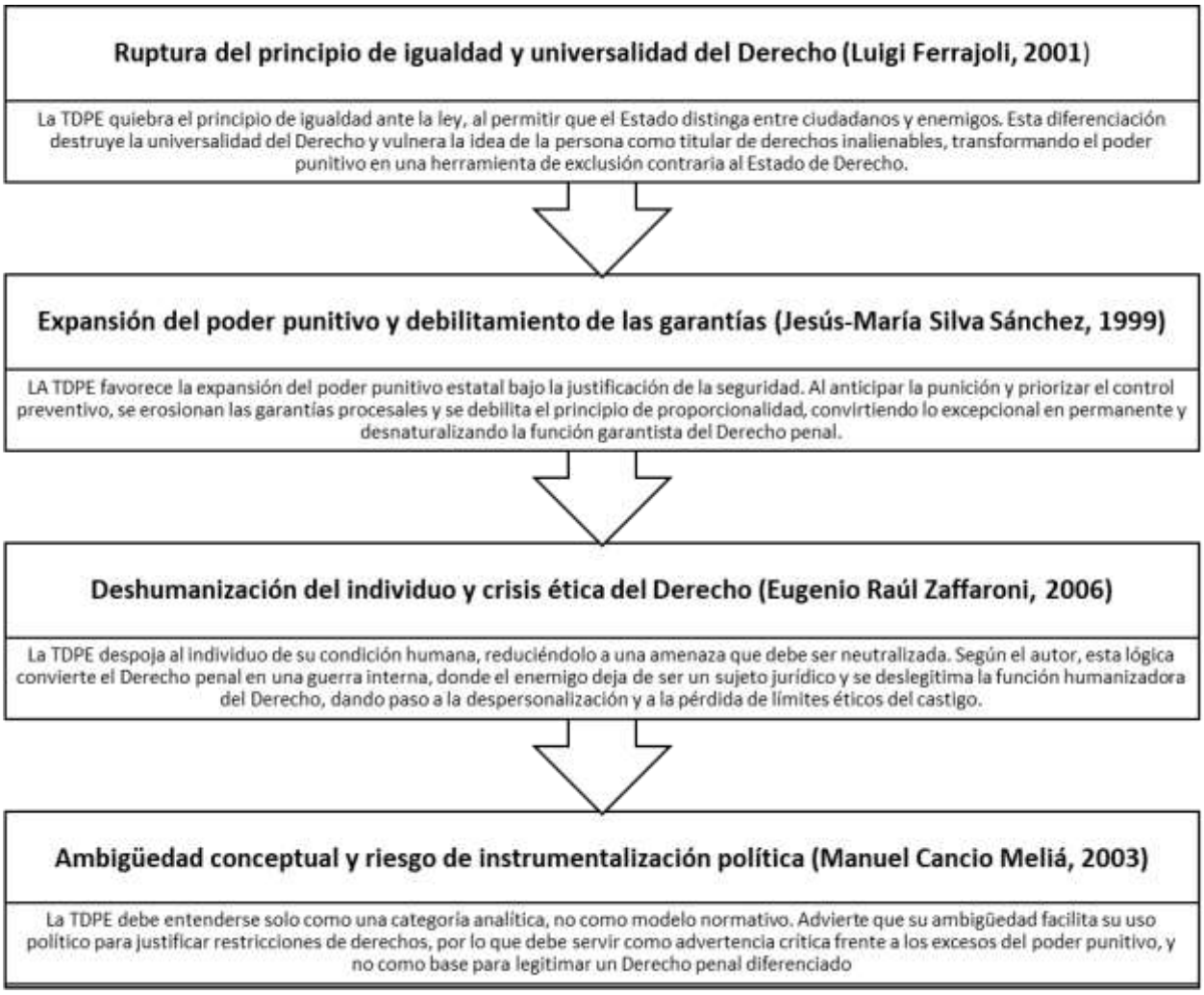


Fuente: Elaboración propia con base en (Almeyda, 2015).

Las objeciones formuladas frente a esta concepción no son unívocas, sino que con miramientos del trabajo se han condensado en cuatro perspectivas principales:

Figura 21.

Cuatro posturas críticas frente al TDPE.



Fuente: Elaboración propia con base en (Almeyda, 2015).

Las críticas de Ferrajoli, Silva Sánchez, Zaffaroni y Cancio Meliá coinciden en un indicador crucial: la TDPE pretende proteger el sistema jurídico, poniendo en riesgo los propios fundamentos del Estado de Derecho. Ferrajoli alerta sobre la desigualdad y la pérdida de universalidad del derecho; Silva sobre la expansión del castigo y la erosión de garantías; Zaffaroni

sobre la deshumanización de sujeto frente a la categoría de enemigo; y Cancio Meliá sobre la ambigüedad teórica y el riesgo de uso político del concepto.

En conjunto, esas críticas no solo cuestionan la legitimidad del modelo de Jakobs, sino que reafirman la necesidad de un Derecho Penal garantista capaz de responder a los desafíos contemporáneos sin renunciar a su esencia: la dignidad humana y la vigencia universal de la ley.

Teniendo en cuenta todo lo expuesto a lo largo del capítulo y a partir de las observaciones realizadas sobre la configuración, alcances y críticas de la TDPE, se procede a sistematizar los aspectos esenciales del modelo en consideración a sus fundamentos teórico: https://docs.google.com/spreadsheets/d/1iOI6dUN6RR9xWH8HnKCkNVDx_oiGXptHM8rkKq75NhI/edit?usp=sharing

Este ejercicio permitirá examinar si las premisas planteadas por Jakobs encuentran una manifestación material en la práctica jurídico-penal contemporánea, es decir, si la TDPE trasciende el plano conceptual para reflejarse en el marco jurídico colombiano, revelando su aplicación efectiva dentro del sistema penal.

En síntesis, la sistematización de los fundamentos teóricos de la TDPE visibiliza el escenario previsible de una ruptura del pacto social por parte del enemigo; donde el Estado buscar restaurar un equilibrio a partir de la neutralización, siendo una expresión coherente de una concepción sistémica del derecho, orientada a preservar la seguridad y la estabilidad del orden social.

Bajo esta lógica, el TDig sucede como una forma contemporánea de dicho enemigo sistémico, cuya manifestación en el Ciberespacio supone una lucha contra las estructuras normativas y supone un impedimento de los elementos básicos de la convivencia.

Esto hace que sea tratado a la luz del análisis de la TDPE y dentro del concepto de la sociedad del riesgo, donde algunos de los peligros no son solo físicos, sino que son ya tecnológicos, simbólicos y globales.

2.3. Capítulo III. Aplicación del Derecho Penal del Enemigo al tratamiento del Terrorismo Digital en Colombia.

2.3.1. El Terrorismo Digital y su vinculación con el Derecho Penal del Enemigo en la sociedad del riesgo.

La figura del terrorismo tradicional deriva de un campo excepcional de la esfera del delito; pues su naturaleza implica una violencia singularmente diseñada para subvertir el orden, influir en la política y sembrar el terror en sociedad; debilitando así el pacto social.

El fenómeno se sitúa más allá del Derecho Penal clásico; ya que busca destruir el contrato social vigente al no servir a sus intereses. De esta manera, el terrorismo actúa como acto comunicativo al utilizar la violencia directa como medio de transmisión simbólica orientada a infundir terror en la población-apartada de toda benevolencia del DIH- con el fin de aniquilar el orden político vigente.

Su esencia, no obedece a un delito ordinario sino a una amenaza estructural "sui generis" cuyo objetivo está en el declive del tejido del orden constitucional que erige un sistema, por lo que permite justificar medidas extraordinarias por parte del Estado en aras de proteger a la sociedad ante un posible riesgo a gran escala.

Al existir un abandono al proyecto en comunidad de manera voluntaria-por parte de quienes hacen parte de organizaciones criminales que se dirigen a materializar este fenómeno- cualquiera de sus integrantes ya ostentan un rótulo de "enemigo interno".

Como sostiene Jakobs (2003), este tipo de sujetos no prestan la garantía cognitiva mínima necesaria para ser tratados como personas, lo que significa que han abandonado el Derecho Penal ciudadano y han de situarse dentro del marco del Derecho Penal del Enemigo (DPE).

El jurista Isidoro Aramburo (2015) confirma esta aseveración, al considerar que el esquema propio de la TDPE está supeditado a un tipo criminal específico que actúa de forma persistente y representa un peligro constante: el terrorismo que aunque no el único, es el máximo exponente.

Continuando con este razonamiento, para Pablo Elías González Monguí (2019) los individuos peligrosos o quienes materializan la figura del enemigo:

> (...) serían aquellos que pertenecen a la criminalidad económica, al terrorismo (Bernal Castro, 2018), a la criminalidad organizada que se expresa como delincuencia común, al narcotráfico (González Monguí y Villarreal Correcha, 2015), a la delincuencia política y al concierto para delinquir. También podrían caber otros que actúan individualmente como los delincuentes sexuales y los autores de "otras infracciones penales peligrosas" , que el autor deja como abiertas, posiblemente para que dadas las circunstancias se califiquen como potencialmente realizables por éstos (p. 1074).

Si se sigue con este argumento, el terrorismo daría pie a la aplicación de un Derecho Penal de guerra o de supervivencia, cuyo objetivo ya no sería el de la reeducación o la reinserción, sino tan solo el evitar el peligro, la neutralización preventiva del mismo.

Por lo tanto, puede afirmarse que el terrorismo tradicional es la manifestación practica (la especie) que describe y sustenta la TDPE ofrecida por Jakobs (el género). Este fenómeno, es precisamente a lo que el profesor alemán se refiere cuando advierte que los sistemas garantistas penales contemporáneos ya aplican prácticas propias de esta teoría; podría decirse "por debajo de la mesa".

Es menester destacar, que el autor no pretende promover este derecho, por el contrario considera deseable su inexistencia; sin embargo, su objetivo se encauza en la descripción de un comportamiento real del sistema, pues aunque los Estados se jactan de aplicar un Derecho Penal del ciudadano, en la práctica coexisten con un Derecho Penal encubierto dirigido a la neutralización de quienes perciben como peligrosos.

En síntesis, el terrorismo representa el ejemplo paradigmático que explica la razón de ser de la TDPE: un derecho orientado al control del peligro más que a la juridicidad, que transforma al ciudadano en objeto de neutralización-no persona- cuando decide romper definitivamente su vínculo con el Derecho y la seguridad pública.

En verbigracia, a partir de los atentados del 11 de septiembre de 2001, el terrorismo, que antes se consolidaba en ámbitos locales, adquirió una dimensión internacional, lo que produjo una respuesta por parte de la comunidad internacional concentrada en la doctrina norteamericana y avalado por la Naciones Unidas.

En aras de contrarrestar estos actos, se creó un ordenamiento jurídico anticipado, encarnado en el ámbito penal orientado a la gestión del peligro, donde el Estado asume una función eminentemente preventiva. La legitimidad del actuar del Estado se mide por su capacidad de neutralizar amenazas antes de que se materialicen, una expresión clara de la TDPE.

En esa misma línea preventiva frente a riesgos a escala global y una vez comprendido el impacto global del terrorismo, resulta esencial abordar el papel desempeñado por la ONU, a través del Consejo de Seguridad como organismo encargado del mantenimiento de la paz y la seguridad internacional, el cual ha impartido resoluciones vinculantes para los Estados miembros, frente a la expansión del terrorismo.

Su expansión en gran medida se debe al ámbito digital, amplificando una tendencia que la comunidad internacional busca anticipar y ejercer control sobre el riesgo potencial a partir de un marco de resoluciones desarrolladas por este organismo en materia de cooperación para combatir el terrorismo. Entre las principales disposiciones desarrolladas por dicho Consejo en esta materia se destacan:

Figura 22.

Resoluciones y Programas de la ONU en la Lucha contra el Terrorismo "Digital"

Fuente: Esquema propio con base en la información proporcionada por el Consejo de Seguridad de las Naciones Unidas. (2021).

Todas las resoluciones referidas, comparten una condena en contra del fenómeno del terrorismo, en todas su manifestaciones, al ser considerado como una amenaza a la paz y a la seguridad internacional, su finalidad es imponer obligaciones a los Estados miembros como Colombia, para prevenir, reprimir y combatir el terrorismo.

En las resoluciones se observa por parte del Consejo de Seguridad un creciente énfasis en la prevención y neutralización de un enemigo a nivel internacional "el terrorista", en conjunto con una serie de sanciones para debilitar la capacidad operativa de los grupos terroristas, antes de que

se cometan actos violentos se alinea con la lógica de adelantar la punibilidad y centrarse en la peligrosidad del "enemigo", muchas veces basadas en percepciones subjetivas del "enemigo" y justificadas por el miedo a amenazas potenciales como el uso del internet o herramientas tecnológicas.

Esta mutación del modelo punitivo no puede comprenderse sin recurrir a la teoría de la sociedad del riesgo de Ulrich Beck (1986), quien advierte que la sociedades actuales viven de manera consciente y continúa de la existencia del peligro; cuyo origen no son los factores externos como la naturaleza, sino las propias acciones internas de la especie en aras de consolidar su progreso.

Esta situación es denominada como “sociedad de riesgo”, donde el riesgo deja de ser la excepción a la regla y se convierte en una condición determinante de la vida en sociedad. La evolución del ser humano en sociedad se encuentra ligada al avance técnico y científico, el cual es amplificado por el fenómeno de la globalización que deriva en una interdependencia entre los Estados, en conjunto con avances de las nuevas tecnologías.

De acuerdo con la doctrinante Luz Mary Rincón Romero (2016):

> La sociedad del riesgo ayuda a la consolidación y nacimiento del derecho penal del enemigo, en el sentido que esta produce la flexibilización de las normas de imputación penal, dejando de lado aspectos elementales de la misma, adecuando la técnica legislativa de crear una norma penal que castigue actos preparatorios (p. 307).

Bajo este enfoque, los subsistemas que permiten la materialización de la convivencia social, se encuentran en un estado de vulnerabilidad permanente; ante el continuo surgimiento de avances que se constituyen como amenazas inminentes y difusas para el entorno.

Según la jurista Natalia Andrea Bravo Peña (2007) “La sociedad del riesgo es consecuencia directa del temor al exterminio global. Tememos aquello que nos puede afectar a todos, no aquello que se puede sectorizar. Hoy los temores son globales, el riesgo ya no es para algunos sino que para todos” (p.86).

De allí que, el eje de la vida social, lejos de enfocarse en la búsqueda de un bienestar común, se encuentra enfocado en la administración del riesgo, pues lejos de sucumbir ante este fenómeno, se busca enfrentarlo desarrollando mecanismos para preservar el orden colectivo, cuyo protagonista es el Derecho Penal.

Tal como señala Hassemer (1991), dicha demanda de seguridad deriva en un proceso de expansión del Derecho Penal, puesto que sirve como una forma de dar seguridad a la comunidad frente a los miedos que identifican a la población.

El resultado es la configuración de un Derecho Penal simbólico cuyo fin es más preventivo y de control que de justicia. En esta misma línea, Mendoza Buergo (2001) plantea tres rasgos principales que conforman esta nueva forma de entender el Derecho Penal:

Figura 23.

Derecho Penal en la sociedad del riesgo.

Fuente: Elaboración propia con base en Mendoza (2001)

Así, el terrorismo —como expresión extrema de riesgo político y existencial— se integra a ese imaginario de amenazas constantes y difusas, cuyo combate se hace a partir de estrategias de control de riesgo ante la estabilidad colectiva que justifica su tratamiento diferenciado. Esta perspectiva está determinada por varios fundamentos teóricos de la TDPE, entre ellos la prevención absoluta ante amenazas futuras y anticipación punitiva.

Por consiguiente, el terrorismo se convierte en un estímulo que enlaza al Derecho Penal con la teoría de la sociedad del riesgo: un derecho de prevención de riesgos futuros. Un modelo que identifica y neutraliza el peligro y lo anticipa antes de que se produzca. Bajo esta lógica, el Estado gestiona la incertidumbre no solo con la sanción, sino que vigila, controla, previene.

En la situación actual, este mismo razonamiento de anticipación y gestión del riesgo se proyecta al Ciberespacio, un entorno que amplía las fronteras del conflicto, multiplicando las fuentes de amenaza en el ámbito virtual. En el Ciberespacio, ciudadano y enemigo se diluyen; ya que el actuar se representa por el anonimato, la transnacionalidad y la descentralización provocando un impacto considerable.

El Ciberespacio en su ámbito virtual, (como se observó en el marco teórico del primer capítulo) ha dejado se ser un mero entorno tecnológico aislado de la sociedad; por el contrario, en la actualidad convergen dinámicas sociales, económicas, políticas y culturales de alcance global. No obstante, pese a su potencial como herramienta de progreso, ha contribuido a ser un territorio de vulnerabilidad que escapa de la regulación de los Estados, por su novedad.

Manuel Castells (2009) en su obra "*La era de la información",* señala que el poder no se ejerce sobre territorios físicos, sino en flujos de información del plano virtual. Este desplazamiento implica a su vez un traslado del conflicto a este nuevo ámbito; representando una nueva forma de riesgo y vulnerabilidad, que trascienden las fronteras físicas del Estado y desafían su capacidad de control.

Por consiguiente, la naturaleza del Ciberespacio genera nuevos escenarios de riesgo al ser una extensión de la realidad, pero sin las barreras jurídicas que estructuran el mundo material, pues

a pesar de ser una infraestructura esencial existe una ausencia de regulación efectiva, favoreciendo el surgimiento de nuevas formas de criminalidad o la reproducción fidedigna de esta en el entorno digital.

Ahora, con la pandemia COVID 19, coadyuvo a que existirá un incremento sin precedentes de la dependencia de la TICs, debido a que " supuso un nuevo acelerón en la digitalización de la sociedad, traducido en el crecimiento del uso de internet en general y de las redes sociales en particular"(Cardeño, 2021, p.102).

Lo anterior, fue gracias a que para mitigar el impacto socioeconómico de la crisis sanitaria se desarrolló una virtualización forzada que magnificó la exposición de las personas a este riesgo, produciendo nuevas vulnerabilidades y oportunidades para la comisión de delitos cibernéticos, exacerbando la necesidad de respuestas penales adaptadas a este nuevo entorno digital.

La expansión del ciberdelito comenzó a tensar el delito común y evolucionó en prácticas más agresivas desestabilizadoras del pacto social, logrando un nuevo escenario operativo para grupos terroristas que potencian sus estrategias tradicionales desde el entorno virtual reproduciendo la lógica del miedo con mayor eficacia, rapidez y cobertura.

Con esto en mente, en el marco de la sociedad de la información, el terrorismo cibernético surge como una categoría amplia que agrupa las nuevas expresiones del terrorismo en el entorno tecnológico; sin embargo, su margen es tan amplio que su concepto se delimito en dos expresiones: el terrorismo informático y el Terrorismo Digital (TDig) (véase Figura 10)

Dentro del margen aplicable, el TDig, no pretende socavar la infraestructura tecnológica. Se encamina a debilitar los subsistemas simbólicos que sustentan la convivencia tales como la confianza, la verdad y la legitimidad de las instituciones a través de redes sociales, medios digitales, flujos digitales de información que mueve la gran red (internet), convirtiendo el lenguaje en un instrumento de poder y el espacio comunicativo virtual en un escenario de conflicto.

El TDig, representa una mutación ontológica del riesgo, en atención a que el escenario ha cambiado; ya que, su objetivo no es el daño físico inmediato, sino el colapso del vínculo social del

propio tejido colectivo desde la guerra psicológica y cultural a partir de la instrumentalización de las plataformas, donde la agresión no se mide en bajas materiales, sino en pérdida de confianza comunicativa.

El terrorista digital no reconoce el orden jurídico, no se somete a las reglas del discurso democrático y opera desde la negación de la expectativa normativa, no se está ante un infractor común, sino un actor que utiliza la libertad comunicativa y tecnológica —los propios medios contemporáneos— para destruir sus cimientos, su manifestación natural: representa la antítesis del ciudadano normativo y encarna la ruptura entre el Derecho y la conducta socialmente esperada.

En este orden de ideas, se podría afirmar sin ningún tipo de duda que el TDig es, por así decirlo, una representación del TDPE; no porque la normatividad lo establezca sino porque su práctica encarna la lógica de profesor Jakobs, que es aquella por la que el sujeto se autoexcluye del pacto normativo, renuncia a ser un ciudadano y se convierte en un riesgo permanente.

El TDig además de ser una amenaza revela los propios límites del Derecho Penal en la actualidad, por la que el Estado pasa a preguntarse su capacidad de respuesta ante quienes no reconocen su legitimidad dentro del Ciberespacio.

Entonces, la diferencia entre el terrorismo tradicional y el digital radica, por un lado, en el medio y no en las características propias de lo que se consideraría el terrorismo en sí mismo, al compartir el mismo propósito: negar el orden jurídico como forma de organización social y sustituirlo por el caos o el miedo como forma de control.

Partiendo de este marco, donde Terrorismo Digital (TDig) es una expansión del radio de acción del terrorismo en plataformas virtuales, siéndole inherente la encarnación de la figura del enemigo al ser aquel que niega el pacto normativo y busca desestructurar la convivencia mediante el uso del Ciberespacio. Se hace necesario examinar cómo el Estado colombiano ha intentado afrontar este fenómeno dentro de su propio ordenamiento jurídico.

2.3.2. Marco jurídico y político del Terrorismo Digital en Colombia.

Como punto de partida, se advierte que Colombia no ha quedado al margen del desarrollo del terrorismo y su adaptación al Ciberespacio; para ello se analizara el contexto del terrorismo tradicional en territorio colombiano y su normatividad frente a los nuevos avances tecnológicos que han alzado el ciberterrorismo, en especial lo que comprende al objeto de estudio el TDig.

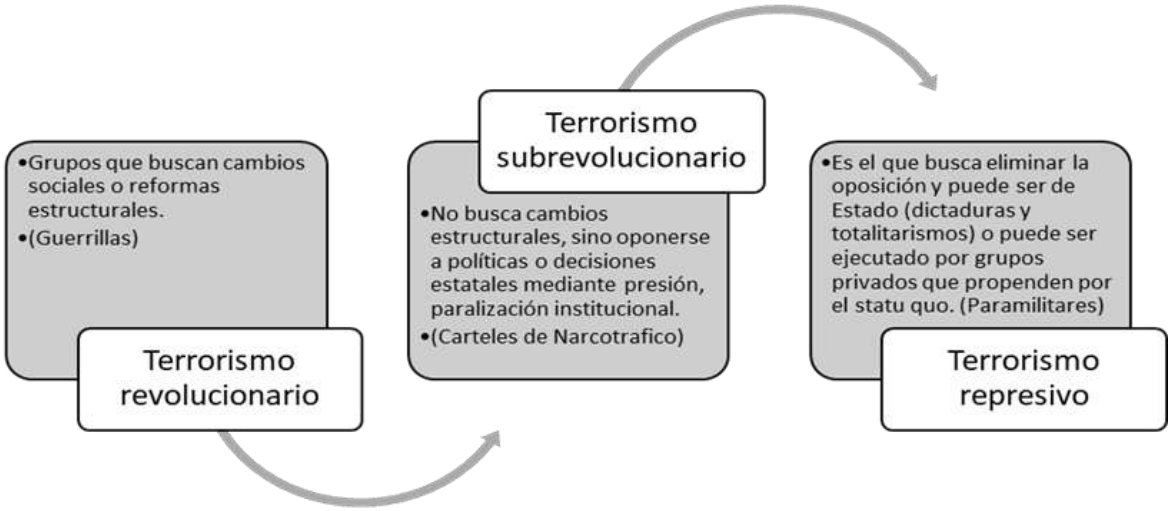
La historia de Colombia se ha encontrado enlazada por un prolongado ciclo de violencia estructural derivado del conflicto armado interno, narcotráfico y pugnas por el poder que han devastado el tejido social y moral del país; cuyas principales víctimas, han sido los pobladores no combatientes y el medio ambiente.

El terrorismo en este contexto, se consolido desde los años setenta como una expresión de violencia organizada, utilizada por grupos insurgentes, privados y organizaciones criminales, con el objetivo de desplegar una estrategia que permitiera a través del miedo ejercer control político/territorial o presión sobre el Estado colombiano, logrando un impacto directo frente a la seguridad nacional y la estabilidad social.

Según Armando Borrero Mansilla (2010) quien retoma la clasificación que le da Paul Wilkinson, el terrorismo en Colombia se ha encontrado desarrollado dentro de tres fases representativas ((Muñoz Sánchez, Pontvianne & Álvarez Posada, 2019, p. 84-85)

Figura 24.

Clasificación del terrorismo en Colombia.



Esquema propio con base en la información de (Muñoz Sánchez, Pontvianne & Álvarez Posada, 2019, p. 84-85).

Sin embargo, las fases planteadas distorsionan el concepto de terrorismo, al terminar equiparándolo, en un primer momento, a la figura rebelión; de hecho, esta confusión conceptual, es frecuentemente promovida por el Estado para legitimar sus actuar político.

Conviene precisar que, categorizar bajo una lectura indistinta revoluciones, luchas sociales y terrorismo en un mismo rótulo; permite que los gobiernos en procura de restaurar un orden interno desde un enfoque represivo, comiencen a generar políticas públicas para su restablecer el orden interno, criminalizando ámbitos de disidencia y protesta.

En verbigracia, en el periodo presidencial Julio Cesar Turbay Ayala, inaugura la categoría jurídica del terrorismo, desde una visión tradicional, a partir del Estatuto de Seguridad (Decreto 1923 de 1978) extendiendo su uso a todo tipo de oposición, abriendo paso a la aplicación desproporcionada de estados de excepción que permitía en su momento la Constitución de 1886 (Torres Vásquez, 2015).

Posteriormente, en vigencia del Estatuto, se expide el Código penal de 1980 (Decreto 100 de 1980) tipificando el terrorismo como delito que vulnera el bien jurídico de la seguridad pública, consolidando su implementación punitiva de manera indiscriminada. Esta tendencia continuó durante gobiernos sucesivos, reforzando su aplicación ante cualquier amenaza percibida por el gobierno contra el régimen constitucional (Torres Vásquez, 2015).

Con el gobierno de Virgilio Barco, se aprecia un intento de introducir el famosos Estatuto para la Defensa de la Democracia, cuya esencia buscaba penalizar el terrorismo a partir de un enfoque mixto que planteaba la implementación de mecanismos de negociación con insurgentes, en conjunto con mecanismos punitivos ordinarios frente a los actos terrorista acaecidos por organizaciones criminales. Lineamientos que en la actualidad se siguen ejecutando.

Empero, es con la Constitución de 1991, al establecer un ordenamiento jurídico sólido en la protección de derechos fundamentales fundado en la dignidad humana, en conjunto con el fin de garantizar una convivencia pacífica en un Estado Social de Derecho (ESD), donde la paz es un fin, valor y derecho, que comienza a limitarse la figura del terrorismo.

A partir de lo señalado, el texto constitucional proporcionó un equilibrio entre garantías y seguridad pública que la constitución de 1886 no tenía; de este modo, el terrorismo debía respetar los límites inherentes a los derechos humanos y principios rectores de la carta, alejando su enfoque legalista eminentemente represivo como discrecional. Así, se buscó evitar que la lucha contra el terrorismo continuara con violaciones arbitrarias de garantías.

De igual manera, la constitución al incorporar de manera directa los tratados internacionales referente a derechos humanos y derecho internacional humanitario dentro del bloque de constitucionalidad (artículo 93), sentó las bases para diferenciar el terrorismo del conflicto armado interno, que fue desarrollado de mejor manera con los Acuerdos de la Habana.

De esta forma, el terrorismo se circunscribe en una instrumento o estrategia de impacto psicológico que soslaya el pacto social; en cambio, el conflicto armado interno, aunque violento, es un enfrentamiento prolongado entre el Estado y distintos actores armado que alcanza el umbral del Derecho Internacional Humanitario.

Sin embargo, muy a pesar de este marco garantista, los ataques ocurridos 11 de septiembre de 2001 en las principales ciudades de Estados Unidos, sentó las bases de una política internacional en la lucha del terrorismo auspiciada por el Consejo de Seguridad de la Naciones Unidas y por la Asamblea General.

Colombia al ser un Estado Miembro, fue drásticamente influenciado por la lucha antiterrorista, al punto de que el presidente Andrés Pastrana Arango (1998-2002) "El 27 de noviembre de 2001 en Colombia dio inicio a la estrategia integral contra el terrorismo, denominada: "El Camino hacia la Paz y la Estrategia contra el Terrorismo" (Torres Vásquez, 2015. p. 26) fortaleciendo las redes de seguridad locales, dando un mayor poderío a las fuerzas armadas.

Colombia se alineó con esta tendencia global incorporando a su ordenamiento jurídico tratados internacionales contra la figura del terrorismo; así como, las resoluciones del Consejo de Seguridad de la ONU, con el objetivo de fortalecer su capacidad de prevención, investigación y sanción de este tipo de delitos, asimilando un enfoque preventivo y peligrosista.

Desde este enfoque, el mandato de Álvaro Uribe Vélez reforzó la senda de la respuesta militar y punitiva; endureciendo la gravedad de las sanciones y creando delitos conexos como la financiación del terrorismo, por ejemplo, la política de "Seguridad democrática" como modelo de gobernanza despolitizó al contradictor y agudizó la persecución penal.

El viraje se dio con el gobierno de Juan Manuel Santos, quien propuso la salida negociada del conflicto armado, pero también realizó un giro en la manera de entender jurídicamente la frontera entre terrorismo y conflicto armado interno.

Aun así, los gobiernos que han seguido al de Santos han mantenido la tensión entre uso de la fuerza y el diálogo: el gobierno de Iván Duque retomó el camino de la dureza a partir de un esquema de militarización y el de Gustavo Petro propone una política integral que sostiene el uso del diálogo, el reconocimiento de múltiples actores y la justicia transicional.

En estos dos últimos gobiernos donde los actores terroristas han alcanzado una notable variación en la forma en que han desplegado sus actos gran parte debido a la implementación y el

uso creciente de tecnologías como mensajería cifrada, las redes sociales y la inteligencia artificial ha facilitado que estos grupos armados puedan operar con más sigilo y eficacia.

Esta nueva realidad requiere de una adaptación de las políticas de seguridad y justicia, como el desarrollo de tipificación punitiva ya que el terrorismo no solo se libra en el territorio, sino también en el Ciberespacio.

Continuando con este razonamiento, con la constitucionalización del Derecho Penal y la Ley 599 de 2000**,** el tratamiento del terrorismo en Colombia se reorientó hacia la legalidad y la sistematización de la conducta punible a partir de dos artículos propios de este fenómeno en el conflicto armado interno (artículo 144) y en delitos comunes (artículo 343); los cuales, son escenarios pertenecientes al terrorismo tradicional.

El legislador colombiano, permitió sistematizar una figura que en sus inicios fue discrecional, bajo un tratamiento penal más coherente y preciso recogiendo los elementos propios del terrorismo a nivel internacional, pero es necesario establecer si esta tipificación se adapta a amenazas en entornos digitales.

En primer lugar, se presenta el artículo 144, que determina cuando se está en frente de actos de terrorismo en el contexto de los delitos contra personas y bienes protegidos por el Derecho Internacional Humanitario, es decir dentro del conflicto armado:

Figura 25.

Elementos del Terrorismo en contextos de conflicto armado interno.

Fuente: Elaboración propia en Napkin con base en el artículo 144 de la Ley 599 de 2000.

Como se observa el artículo 144, corresponde a una esfera distinta al delito común, su ubicación obliga a que se encuentre interpretado a luz de los principios del DIH en contexto de conflictos armados, el cual se aplica a cualquier combatiente, incluidos miembros de la Fuerza Pública, quienes serán juzgados por la justicia penal ordinaria en caso de generar la conducta comentada.

Los sujetos pasivos protegidos incluyen a: la población civil, personal médico, religioso, periodistas, combatientes fuera de combate, o bienes protegidos según los Convenios de Ginebra y sus protocolos adicionales; su aplicación requiere de la existencia de un acto con intención de aterrorizar, puede incluir ataques indiscriminados y excesivos, pudiendo concurrir con otros delitos como la perfidia.

Pero su tipología, no contempla ni abarca elementos que permitan perfilarlo en violencia ejercida mediante medio tecnológico, quedando fuera de su alcance punitivo.

Por otro lado, se encuentra el artículo 343, que aplica la figura del terrorismo para delitos comunes, el tipo penal se encuentra ubicado en los delitos contra la seguridad pública; reproduciendo, sin mayores modificaciones, el contenido del artículo 4º del Decreto 2266 de 1991.

Frente al análisis dogmático del tipo penal (art 343), la Corte Suprema de Justicia en su doctrina probable ha generado una interpretación concreta del mismo en diferentes jurisprudencias, manifestando que la conducta punible tipificada busca proteger el bien jurídico de la seguridad pública y requiere para su estructuración que el sujeto no cualificado:

> i) realice una de las conductas alternativas: provocar o mantener en zozobra o terror a la población o parte de ella.
>
> ii) lo cual debe lograr a través de actos que pongan en peligro la vida, la integridad física o la libertad de las personas o las edificaciones o medios de comunicación, transporte, procesamiento o conducción de fluidos o fuerzas motrices y
>
> ii) utilizando para ese fin medios que tengan la capacidad de causar daños (Corte Suprema de Justicia, Sala de Casación Penal, Sentencia SP13290-2014, 2014, M. P. María del Rosario González Muñoz)

El primer aspecto, requiere del elemento subjetivo, sin embargo, el ítem segundo este precepto extiende la tipicidad a conductas que generen un peligro real sobre una gama más extensa de bienes jurídicos.

Así, no solo se protege la vida y la integridad física o la libertad de las personas, sino también infraestructuras clave para el funcionamiento social, como edificaciones, medios de transporte, comunicación y sistemas de conducción de fluidos o energía.

De allí, que dentro de esta tipología (art 343) pueda observarse una redacción que responde a la concepción de un terrorismo tradicional como una amenaza física o directa; empero, el legislador dentro del mismo articulado desarrollo un clausula abierta "valiéndose de medios capaces de causar estragos", que adaptado a una perspectiva contemporánea puede considerarse una aplicación para futuros escenarios cibernéticos.

Sin embargo, la referida cláusula abierta del artículo 343, continúa reproduciendo un anclaje material, toda vez que se requiere de medios con capacidad destructiva tangible; ya que, si bien puede ser tanto una conducta punible de resultado como de peligro real, exige el uso de medios potencialmente lesivos para alcanzar su propósito: infundir temor colectivo.

Esta finalidad sólo se configura si los actos realizados representan un riesgo concreto para las personas o los bienes protegidos por el tipo penal.

Tal como lo advierte Iván González Amado (2007):

> Por lo demás, los ataques digitales no son, por sí mismos, un medio con potencialidad para producir estragos, esto es, "ruina, daño o asolamiento", sino que estos efectos deberán producirse como consecuencia de la afectación de los sistemas informáticos y programas que regulan y controlan algunos medios materiales con los que, ahora sí, podría producirse daños generales a la población o a las condiciones materiales en las que ella desarrolla su vida ordinaria. (p. 41)

En consecuencia, los entornos digitales pueden causar de manera indirecta, pánico o afectar servicios esenciales, pero al desarrollarse en un entorno virtual no se vislumbra ese riesgo concreto que exige la normatividad tradicional por su propia formulación, pretender subsumir conductas que no se encuentran reguladas por este medio implicaría una analogía in malam partem, contrario al principio de legalidad y garantías constitucionales.

Adicionalmente, el parágrafo del artículo 343 contempla un aumento punitivo para cuando esta conducta, se produzca mediante *"llamada telefónica, cinta magnetofónica, video, casete o escrito anónimo",* lo cual constata un retraso frente a la época contemporánea.

Si bien, el legislador a principios del siglo XX se valió de los medios de comunicación social tradicionales que tenía a su disposición, no supo anticipar la existencia de los espacios digitales y de las plataformas interactivas o de las redes sociales como nuevos espacios de promoción del fenómeno, quedando rezagado y generando un vacío normativo sustantivo.

En cuanto, al artículo 344 que contiene circunstancia de agravación punitiva aplicables a los tipos previstos por el terrorismo común, elevan la pena determinadas circunstancias que pueden atender al terrorismo clásico; pero en cuanto a una medida que describa algún medio digital, no lo abarca, continúa anclada a los medios con capacidad destructiva tangible.

Por otro lado, frente al artículo 345 que trae a colación la práctica del financiamiento al terrorismo- conducta peligrosista- su enfoque es eminente económico y material, se considera insuficiente ante las nuevas formas modernas de financiamiento digital (criptomonedas, crowdfunding en línea, desvío de activos virtuales o lavado a través de plataformas digitales).

Para finalizar, el artículo 348 dirigida a instigación a delinquir con fines terroristas, podría abarcar parcialmente algunas estrategias del TDig, como: la propaganda extremista, la radicalización en línea o la incitación de violencia en redes; aunque su redacción encuentra dos limitaciones no diferencia ni regula expresamente el uso de medios tecnológicos como instrumentos de adoctrinamiento o difusión ideológica.

Figura 26.

El Terrorismo Digital (TDig) en el código Penal Colombiano.

Fuente: Elaboración propia en Napkin con base en la Ley 599 de 2000.

Con la expedición de la Ley 1273 de 2009, la cual hace referencia a aspectos de la criminalidad digital, incorporando los bien conocidos ciberdelitos, específicamente a partir de la adición del Título VII BIS al Código Penal, el cual se denomina: “De los delitos informáticos y la protección de la información y de los datos” en el cual se tipifican las siguientes conductas: acceso

abusivo a un sistema informático (art. 269A), interceptación de datos (269B), obstaculización ilegítima de sistemas (269C) y violación de datos personales (269F), entre otros.

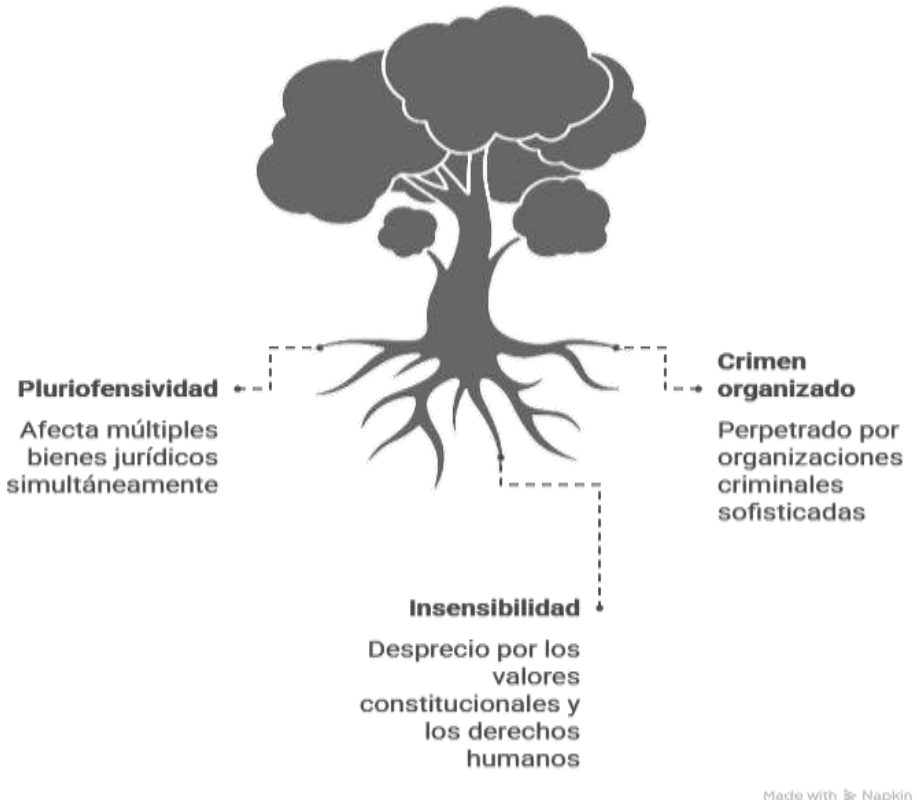
Ningún tipo penal mencionado contemplados tanto en Título VII BIS y Titulo XII (art. 343, 344, 345, 348) del Código Penal es capaz de dar cuenta de la complejidad del fenómeno del Terrorismo Digital (TDig), ni permiten abordar de manera integrada sus formas de manifestación, tales como la radicalización en línea, el adoctrinamiento, la propaganda extremista o la coordinación de actos de violencia.

En materia jurisprudencial, desde la perspectiva constitucional, la Sentencia de la Corte Constitucional C-127 de 1993 (M.P. Alejandro Martinez Caballero) considera que el tipo penal constituye un delito autónomo y dinámico, legitimando dentro del ordenamiento jurídico penal tipos penales abiertos que permite al legislador responder ante su condición fluctuante, siempre que se mantenga la legalidad y proporcionalidad.

De igual manera, dispone el alto tribunal que el delito de terrorismo busca proteger el valor fundante de la paz, la convivencia pacífica y vigencia de un orden justo, por lo que es un tipo penal de carácter pluriofensivo, dado que protege diversos bienes jurídicos. Bajo esta dinámica la Corte edifica 3 características esenciales:

Figura 27.

Características del Terrorismo en la jurisprudencia Colombiana.



Fuente: Elaboración propia en Napkin, con información tomada de con base en Corte Constitucional, Sentencia C-127 de 1993, M. P. Alejandro Martínez Caballero.

Posteriormente, en Sentencia C-073 de 2010 (M.P.: Humberto Antonio Sierra Porto), la Corte reafirmo la exclusión del tipo penal del terrorismo frente al aprovechamiento de mecanismos punitivos excluyentes (como el reconocimiento de beneficios penales en forma de reducción de pena o de libertad condicional).

Respecto de delitos que transgreden la seguridad pública y la convivencia colectiva, el legislador posee un margen de configuración normativa amplio, incluso sustentado en compromisos internacionales que adquirió Colombia en el ámbito de la lucha contra el terrorismo.

Finalmente, la Corte Suprema de Justicia delimita el bien jurídico del terrorismo amparado por el artículo 343, bajo el precepto de la seguridad pública y su marco jurisprudencial entro su labor en la definición y aplicación del tipo penal.

En sentencia, SP13290-2014 (M.P. María del Rosario González Muñoz) realiza un análisis dogmático del tipo penal del terremoto artículo 343 manifestando los siguientes aspectos transcendentales para su identificación:

1. *Sujeto activo-pasivo:* El sujeto activo del terrorismo es indeterminado, es decir no exige una cualificación, en cuanto, al sujeto pasivo, es el colectivo e indeterminado, la víctima no es una persona concreta es la población general o parte de ella.
2. *Tipo Objetivo:* Posee dos verbos rectores "provocar" o "mantener" en estado de zozobra o terror a la población o a una parte de ella, su modificación se encuentra en suprimir el móvil del autor, lo que implica su verificación fáctica.
    - Zozobra: Estado colectivo de intranquilidad o angustia.
    - Terror: alude al miedo, pánico, temor, etc.

    Por otro lado, la conducta típica obedece a un delito de resultado de peligro concreto, donde es indispensable que la acción genera una afectación en el marco de "zozobra" o "terror", para ello debe utilizarse un medio capaz de causar estragos (con potencial real de destrucción).
3. *Resultado y relación teleológica*: Debe existir una conexión entre la conducta y el fin que persigue el tipo penal. Frente al caso, es indispensable la relación entre la acción peligrosa y el efecto psicológico; en otras palabra el acto violento debe producir pánico colectivo bajo un estado de "zozobra" o "terror" a través de medios p capaces de causar estragos. Bajo este referente, es un delito de resultado de peligro concreto.
4. *Bien jurídico protegido*: Para la Corte Suprema de Justicia si bien es un delito pluriofensivo, su núcleo protector se encuentra en la seguridad pública.
5. *Tipicidad Objetiva*. Debe probarse que la conducta efectivamente pone en peligro los bienes materiales mediante medios capaces de causar estragos.

6. *Antijuridicidad*: En este escalón debe verificar si la conducta lesiono o puso en peligro el bien jurídico de la seguridad pública, pero no requiere en si probar la lesión efectiva, basta con la exposición al riesgo real.
7. *Tipo subjetivo:* Conforme al artículo 21, el terrorismo es un delito doloso, habida cuenta de que exige que el agente conozca y quiera generar zozobra o terror mediante medios idóneos para causar estragos. No admite culpa o preterintencional.
8. *Exclusión de conductas:* No aplica para los actos que se cometen con ocasión al conflicto armado interno, el encargado es el artículo 144 de mismo código penal.

Del estudio dogmático presentado se concluye que el tratamiento jurídico del terrorismo se mantiene dentro de un enfoque clásico, reducido a la acción violenta, el medio empleado y la capacidad de generar un estado de zozobra o terror de manera colectiva. De ahí, se entiende este fenómeno como una amenaza para el Estado y la sociedad.

De esta manera, tanto la Corte Constitucional como la Corte Suprema de Justicia han elegido una óptica punitiva y preventiva, en función de mantener el orden público de proteger a la población civil y de hacer frente a las obligaciones internacionales del Estado en la lucha contra el terrorismo.

En conclusión, el contexto colombiano no existe una regulación penal expresa ni sistemática del fenómeno del TDig, el cual se puede definir como una amenaza creciente que trae consigo la confluencia de lo delictivo, lo ideológico y lo tecnológico.

Como en muchos otros Estados, la respuesta jurídica ha sido reactiva y fragmentada, dejando amplios y peligrosos vacíos frente un problema que opera en contextos descentralizados y cambiantes como es el Ciberespacio.

El TDig constituye una amenaza que ha superado los marcos del Derecho Penal tradicional. Ante la ausencia de un tipo penal que recoja de manera integral sus manifestaciones en Colombia; es menester dirigirse a la política pública que se ha desarrollado del tema, que a diferencia de las normas penales que operan de manera reactiva, las políticas tienen un carácter preventivo,

estratégico y coordinador y esto, resulta esencial en escenarios con una amenaza difusa, descentralizada y tecnológica, del TDig.

Respecto a las políticas, como se ha mencionado quien desarrolla lo atinente al tema es el CONPES (Consejo Nacional de Política Económica y Social) los cuales elaboran instrumentos de planeación estratégica de políticas del Estado colombiano necesarias para su desarrollo; pero en particular, políticas dirigidas a la seguridad, la defensa, la tecnología y la educación, configurando una respuesta preventiva y estructural frente a riesgos emergentes.

Es preciso determinar que los documentos CONPES no regulan directamente conductas como el TDig, pero sí integran una zona donde el Estado reconoce y gestiona amenazas derivadas del Ciberespacio que afectan la seguridad nacional, cumpliendo una función tanto de prevención como de mitigación a partir de definir líneas de acción institucional, identificar variables estructurales y fortalecer capacidades de defensa.

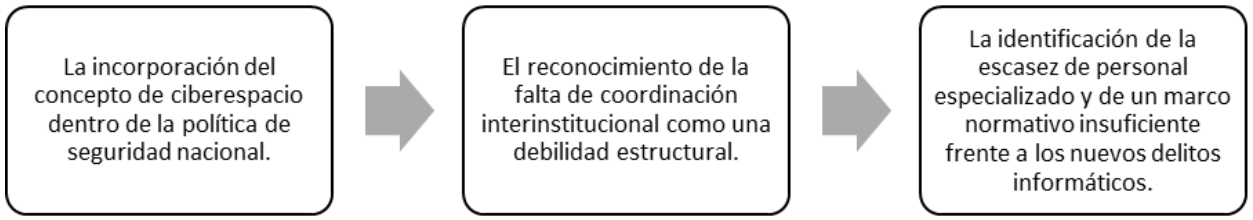
De esta manera actúa como mecanismo anticipatorio.

El Estado colombiano ha adoptado documentos CONPES sobre ciberseguridad, como el CONPES 3701 de 2011 o el 3854 de 2016, dichos documentos fueron desarrollados en el primer capítulo de este trabajo, sin embargo, se debe destacar que fueron los primeros pilares que comenzaron a edificar la política nacional de ciberseguridad y seguridad digital

El CONPES 3701 de 2011 titulado *Política de Ciberseguridad y Ciberdefensa*, es el documento pionero que consolidó una respuesta institucional ante amenazas informáticas, su objetivo buscaba fortalecer al Estado frente a la nueva dinámica de vulnerabilidad tecnológica para esa época, promoviendo la creación de instancias especializada (véase Figura 5) sus principales aportes fueron:

Figura 28.

Aportes Conpes 3701 de 2011.



Fuente: Elaboración propia con base en Consejo Nacional de Política Económica y Social (2011). Documento CONPES 3701.

Por su parte, el CONPES 3854 de 2016 *Política nacional de seguridad digital,* supuso una reformulación de la política, su enfoque no era la ciberdefensa o ciberseguridad, se encauzaba hacia una seguridad digital, adoptando mecanismos de gestión del riesgo, confianza en la línea como ejes estratégicos.

De sus aportes más importantes, fue el reconocimiento de que el entorno digital es dinámico, se encuentra en constante transformación y exige respuestas articuladas.

El documento no menciona el TDig; no obstante, la manera como establece la gestión del riesgo y la lógica de la protección sistémica, formaliza las bases conceptuales para ser capaz de comprender cómo el Estado colombiano empezó a preparar el camino para una forma más sofisticada de amenaza híbrida, en donde la información y la comunicación empiezan a entenderse como una herramienta del poder y del control social.

Dado esto, los CONPES de 2016 en adelante dirigidos al margen de amenazas en el Ciberespacio, los cuales son: CONPES de 3995 de 2020 y CONPES 4144 de 2025, revisten un interés analítico bastante considerable, pues tienen la posibilidad de ser examinados a la luz de lo expuesto por la TDPE.

A través de la aplicación de una matriz analítica generada en el segundo capítulo, se identificará si los CONPES mencionados empiezan a producir fenómenos de prevención

anticipada, expansión de la intervención estatal o excepcionalidad normativa propias del TDPE, en lugar de conservar el enfoque garantista que enmarca las políticas públicas ajustadas a las reglas del Estado Social de Derecho (ESD).

Así mismo, un análisis de esta naturaleza permite dar cuenta de ciertas tendencias vinculadas a la lógica de procesamiento del TDig, en atención a que alguna de las políticas públicas examinadas –implícitamente– aplica estrategias de control, vigilancia o disuasión propias de los escenarios en los que el Ciberespacio se considera un espacio de riesgo potencial o de amenaza a la seguridad nacional.

De tal forma que el examen de los CONPES de 2020 a 2025 a la luz de la TDPE permitirá comprobar si el Estado colombiano avanza hacia una gestión preventiva de amenazas digitales.

2.3.3. Aplicación de la matriz del Derecho Penal del Enemigo al tratamiento jurídico-penal del Terrorismo Digital (2020 a 2025).

El periodo 2020–2025 representa un punto de inflexión para la política de seguridad digital de Colombia ya que, tras la pandemia del COVID-19, la acelerada digitalización de la vida social, económica y estatal amplió las situaciones de riesgo en el Ciberespacio, forzando al Estado a elevar su capacidad de prevención, de vigilancia y de control.

En este marco, los documentos CONPES elaborados en dicho periodo continúan profundizando la evolución de los de 2011 y 2016 hacia una forma más amplia de la seguridad digital, centrada en la prevención, resiliencia y cooperación interinstitucional, profundizando la transición de una ciberseguridad técnica hacia una seguridad digital estratégica.

El objetivo de este apartado es analizar los CONPES 3995 de 2020 y 4144 de 2025 a través de los fundamentos teóricos que derivan de la TDPE con el fin de comprobar el grado de desarrollo de los elementos de prevención, control o anticipación que se pueden encontrar en dicha política.

- CONPES 3995 de 2020: Política Nacional De Confianza Y Seguridad Digital.

El presente documento nace como consecuencia de un contexto mundial cambiante en lo social, adicional a un cambio tecnológico acelerado; en el que el uso del internet, la acumulación de los datos de carácter personal en línea o la dependencia de las infraestructuras informáticas nuevas, incorporan en la actualidad nuevos riesgos.

Su implementación en julio del 2020 no fue casual: las circunstancias corresponden a una respuesta forzada de la crisis sanitaria en salud (COVID-19) que derivó en la consolidación de una digitalización forzada en actividades cotidianas como: la educación, el trabajo, el comercio, la administración pública.

Lo anterior, reveló la vulnerabilidad del entorno digital y la necesidad de fortalecer las capacidades de las instituciones para proteger la información y los derechos de los usuarios. En este contexto, el Gobierno de Colombia reconoció la urgencia de adoptar un modelo centrado en la confianza digital, más allá de un enfoque centrado en la ciberseguridad técnica.

El documento parte del supuesto de que la seguridad en el entorno digital no es solo evitar el delito informático, sino que debe garantizar un entorno en el que las personas puedan participar, interactuar y desarrollarse; de allí que, estableciera un deficiente desarrollo institucional frente a políticas anteriores como el CONPES 3854 aprobado en 2016.

Según el documento CONPES 3995 del 2020**,** frente a este asunto expone:

> Así pues, Colombia dentro de su marco de gobernanza y al carecer de un marco de coordinación de políticas de ciberseguridad no puede lograr una adecuada interacción e identificación entre las diversas entidades alrededor del tema. Lo anterior genera la desarticulación y la duplicación de esfuerzos, así como una baja cohesión y coordinación para dar respuesta a incidentes y a contener amenazas que se den en el entorno digital. (Consejo Nacional de Política Económica y Social, p.25)

Lo anterior, constituye una debilidad latente en materia de seguridad digital que a su vez impacta la confianza del país; razón por la cual, para hacer frente ante este problema, el documento se estructura en cuatro pilares:

Figura 29.

Pilares estratégicos CONPES 3995 de 2020

Fuente: Elaboración propia con base en Consejo Nacional de Política Económica y Social (2020). Documento CONPES 3995.

Estos pilares buscan lograr a partir de un proceso de consolidación, construir un ecosistema digital confiable, seguro y sostenible, a través de la articulación y cooperación de estructuras internas COLCERT, CCP y CCO en intercambio de información técnica y estratégica, fortaleciendo su capacidad de respuesta ante probables incidentes cibernéticos, para mitigar tanto su impacto o prevenirlo en su totalidad.

Ahora, no solo se queda en una articulación interna, a través de la cooperación internacional el país busca en organismos multilaterales y alianzas con otros Estados el intercambio de información y buenas prácticas dentro del Ciberespacio, algo incipiente en CONPES anteriores.

No obstante, su cambio esencial es que se enfoca en una gobernanza digital entre diferentes sectores de la sociedad, pues mientras el CONPES de 2016 se centraba en la seguridad digital, el de 2020 incorpora la noción de confianza digital, entendida como un entorno donde ciudadanos, empresas y Estado pueden interactuar sin temor a riesgos cibernéticos desde la regulación o pautas

que marque el Estado pero también el comportamiento de particulares en el entorno, “la confianza digital es la base de todas y cada una de las interacciones en el futuro digital” (Foro Económico Mundial- FEM, 2018).

En síntesis, se pueden presentar los aportes del CONPES 3995 (2020) en función de tres grandes logros que contrasta respecto de los documentos previos:

- Integrar concepto, seguridad y confianza digital como dos conceptos conciliados y de tal suerte que constituyan bases inseparables sobre el desarrollo tecnológico.
- Fortalecimiento institucional, creando los espacios para que la coordinación y la respuesta frente a riesgos digitales se produzcan bajo un cierto sesgo preventivo.
- Dimensión ciudadana, promover la participación y educación digital como medios para la consolidación de la confianza social en el entorno tecnológico.

El CONPES 3995 de 2020 representa un punto de inflexión para el estudio del tratamiento de amenazas digitales, su estructura y objetivos permiten analizar cómo la política pública adopta herramientas preventivas, coordinadas y de vigilancia que podrían configurar un marco propicio para abordar fenómenos de naturaleza híbrida entre lo tecnológico y lo delictivo.

Hecha esta salvedad, a continuación, se aplica la matriz para identificar si el Estado redefine su relación con el ciudadano frente al riesgo digital, al adoptar estrategias de control y anticipación que pueden incidir, directa o indirectamente, en la esfera punitiva.

Aplicación de Matriz: Pestaña No. 3 denominada “Aplicación CONPES 3995 de 2020” https://docs.google.com/spreadsheets/d/1iOI6dUN6RR9xWH8HnKCkNVDx_oiGXptHM8rkKq75NhI/edit?usp=sharing

Análisis.

El análisis del documento CONPES 3995 de 2020 denominado “*Política Nacional de Confianza y Seguridad Digital*” desde los fundamentos teóricos del TDPE ha puesto de manifiesto

la parcial aplicación del modelo, marcada por una tendencia funcionalista y preventiva de acuerdo al promedio emitido por la matriz, cuyo resultado fue de 2.125.

Si bien el documento no establece sanciones penales, su lenguaje y estructura revelan una racionalidad limitada de la TDPE al articular un modelo de control social preventivo en el que la seguridad digital, la confianza y la gestión del riesgo toman la delantera, en relación con la protección de la persona como sujeto de derechos.

Los resultados de la aplicación de la matriz, indican que el CONPES promueve una racionalidad de orden funcionalista; en otras palabras, el sistema busca preservarse a sí mismo, mediante mecanismos de control como: la educación, vigilancia, la cooperación institucional e internacional. Con el objetivo de supeditar la conducta digital de todos los actores que interactúan en ella garantizando un buen uso para que el sistema se mantenga estable.

Desde el funcionalismo sistémico, el Derecho se orienta a mantener la estabilidad de las expectativas sociales; el CONPES adopta esta lógica al priorizar la continuidad del sistema digital sobre la autonomía individual.

La política se interesa por el mantenimiento de la normalidad y del orden digital, por su concepción de seguridad digital entendida como " la situación de normalidad y de tranquilidad en el entorno digital (Ciberespacio), derivada de la realización de los fines esenciales del Estado" (Consejo Nacional de Política Económica y Social, 2020, p. 44) lo cual, responde al principio funcionalista sistémico de la preservación al trasladar el Ciberespacio a una lógica de control orientada a mantener la normalidad institucional.

De igual manera, se van destilando características de la TDPE, especialmente en la forma en que el Estado neutraliza la amenaza, se anticipa a escenarios de riesgos, e incluso se identifica un lenguaje propio de diferenciación entre sujetos de riesgo y ciudadanos; así como, una lógica de vigilancia y control sobre este último, convirtiéndolos en un riesgo más a gestionar.

En primer lugar, en cuanto a la dicotomía entre ciudadano y enemigo; aunque, el documento no exprese de manera directa el término "enemigo", es claro que dentro del articulado

que existe una diferenciación entre actores confiables "ciudadanos digitales" y aquellos que son "amenazas “o "riesgos ".

El ciudadano digital se comporta como usuario de manera segura, coopera de manera activa y se somete a mecanismos de vigilancia institucionales; por el contrario, existen peligros en abstracto que utilizan y vulneran los sistemas sin permitir la confianza digital, o la expectativa de la norma

. En consecuencia, esta distinción simbólica se articula en una separación entre quienes aseguran la estabilidad del Ciberespacio y quienes la comprometen, reproduciendo el esquema básico de inclusión y exclusión propio de la TDPE.

En segundo lugar, desde el funcionalismo sistémico, se observa que documento privilegia la estabilidad del entorno digital nacional, a partir de conceptos claves como seguridad digital al igual que la confianza digital, como valor estructural del sistema que busca una solidaridad dentro del entorno.

Ambos conceptos se dirigen a mantener la cohesión y el equilibrio social, donde el ciudadano no es un sujeto autónomo, este debe alinearse con las normas colectivas, que desarrolla el Estado.

En tercer lugar, en relación con el Derecho Penal de autor, el documento, no crea sanciones de carácter punitivo, es una política pública; pero a pesar de serlo si establece mecanismos de control, vigilancia y prevención para anticiparse a la amenaza.

Esta vigilancia preventiva no se basa en lo que alguien hizo, sino en lo que podría hacer según su comportamiento o perfil digital.

En cuarto lugar, respecto a la anticipación de la punibilidad, es preciso destacar que esta política tiene como finalidad esencial la prevención; de allí que, la anticipación a la ocurrencia del daño sea el eje de su discurso.

En el caso concreto, no existe un castigo frente a la conducta preparatoria o potencialmente peligrosa, pero si presenta mecanismos institucionales que operan bajo la lógica de la prevención, monitoreo y gestión del riesgo asociado al comportamiento digital de los distintos sujetos que interactúan en el Ciberespacio (intervención temprana).

En continuidad con lo anterior, se prevé la neutralización de amenazas, pues el texto define un conjunto de lineamientos orientados a anticipar riesgos, contrarrestar amenazas inminentes mediante la cooperación de organismos especializados internos y externos, logrando una arquitectura de control y vigilancia constante sobre la sociedad digital.

Desde la perspectiva de la despersonalización del individuo, el documento prioriza el funcionamiento del sistema digital por encima de la autonomía; con ello, el individuo sólo tiene valor en la medida en que contribuye a la "confianza digital" y la "normalidad del Ciberespacio" ya sea por su participación activa o por su comportamiento.

Si bien, el texto no suprime derechos ni el principio de la dignidad humana, sí subordina el comportamiento del ciudadano al Ciberespacio, lo que se traduce en la pérdida de centralidad del ser humano ante la máquina digital.

De ello, se deriva que el documento no elimina los derechos individuales, pero los subordina al interés funcional del sistema digital, reduciendo la centralidad del individuo en la toma de decisiones.

Para finalizar, la excepcionalidad, está dada porque el documento fue emitido en el contexto de la pandemia COVID-19 y en un auge global de ciberataques, circunstancias que intensificaron la sensación de vulnerabilidad y justificaron el fortalecimiento del control digital.

Sin embargo, al no existir un modelo directo de sanción ni una tipificación de la conducta, el documento permanece en el ámbito administrativo y preventivo, no termina de cuajar un modelo punitivo de exclusión.

En consecuencia, el CONPES 3995 (2020) se sitúa en un punto intermedio entre la prevención funcionalista y la tendencia circunstancial de la TDPE. El Estado asume un rol de vigilancia a lo largo de todo el proceso como si buscara proteger el orden digital y la soberanía sin incurrir en la represión directa.

De esta forma, la política de lo posible configura una especie de "Estado preventivo", donde el individuo deja de ser un fin en sí mismo para pasar a ser un medio de estabilidad del sistema.

En cuanto al TDig, la política de confianza y seguridad digital surge en un entorno donde las amenazas informáticas, adquiriendo creciente relevancia, esto al delimitar el concepto de amenaza como:

> (…) posible violación de la seguridad digital que tiene el potencial de ocurrir total o parcialmente en el entorno digital. Se caracteriza por la aparición de una situación donde uno o más actores (externos o internos) adelantan una o varias acciones con la capacidad de alterar una infraestructura física, un sistema de información o la integridad de la información en sí. Estas amenazas pueden darse de manera no premeditada y accidental o, por el contrario, de manera intencional con el fin de causar daño, generar problemas o adelantar una agresión cibernética con el objetivo del propio beneficio o para desestabilizar la población, el territorio y la organización política del Estado (p.42) (Subrayado fuera de texto).

El concepto de amenaza, constituye un primer vestigio al establecer a aquellos actores que realicen acciones capaces de alterar la integridad de la información, incorporando el ámbito simbólico e informativo como espacio vulnerable del Ciberespacio, propio del TDig.

Así, cuando esta alteración se produce de manera intencional; con el fin de causar daño generando una desestabilización de la sociedad, se configura un escenario equiparable al TDig, aunque continue sin piso jurídico.

- CONPES 4144 de 2025: Política Nacional de Inteligencia Artificial.

Bajo el marco de la seguridad digital, el Estado Colombiano ha encontrado un nuevo reto de regulación: La Inteligencia Artificial (IA). En una época caracterizada por la digitalización socioeconómica y la apertura de un extenso flujo de datos en internet, la IA se posiciona como una herramienta estratégica para la innovación y desarrollo social.

Sin embargo, ante una sociedad de riesgo, la implementación de esta herramienta conlleva a nuevos peligros y responsabilidades que para el Estado resulta necesario prever y controlar; razón por la cual el 14 de febrero de 2025 es emitido por el Gobierno de Colombia, el CONPES 4144 de 2025 con el propósito de consolidar una política nacional que impulse el desarrollo y uso ético de la IA como motor de crecimiento económico y bienestar social (Departamento Nacional de Planeación, 2023).

El desarrollo de la tecnología puede ser ambivalente: fuente de desarrollo y conocimiento o vehículo de riesgo; todo depende de la disponibilidad, gobernanza y del uso de los datos de la infraestructura digital a través de la cual discurren.

El documento referenciado, busca promover un empleo responsable de esta nueva tecnología no solo desde un enfoque tradicional, también desde un visión ético-social materializada por la aplicación de principios y derechos fundamentales, generando una hoja de ruta a partir de seis ejes estructurales que se orientan hacia el bienestar colectivo, estos ejes son:

Figura 30.

Ejes Estratégicos del Conpes 4144 de 2025.

Fuente: Elaboración propia con base en el Consejo Nacional de Política Económica y Social (2025). Documento CONPES 4144.

Estos ejes estratégicos consolidan una respuesta estatal para mejorar la capacidad de gobernanza en materia del uso de la IA, puesto que el diagnóstico nacional refleja limitaciones en la implementación, investigación y aprovechamiento de este nuevo sistema, para ello estos ejes se orientan a cerrar brechas, fortalecer la competitivas y garantizar un progreso social en un andamiaje ético de la tecnología en el país.

No obstante, pese a su integralidad en ejes estructurales, la consolidación del documento CONPES de 2025 enfrenta grandes desafíos entre ellos se destacan: la baja capacidad institucional en la periferia, municipios rurales siguen teniendo problemas en acceso de redes, dependencia de empresas extranjeras especialistas en tecnología y sostenibilidad financiera de los programas (Consejo Nacional de Política Económica y Social, 2025).

Ahora bien, frente al tema que ocupa el presente trabajo de investigación, el segundo eje estratégico, comprende los datos o información que navega en la gran red, no son solo insumos técnicos, también son activos estratégicos de carácter público esenciales para la vida en sociedad y para el desarrollo de la IA, puesta que esta última se nutre este flujo informativo.

El documento permite observar la importancia de los datos en la actualidad la cual no está dado solo para generar desarrollo, innovación y competitividad, trasciende a la esfera de protegerlos frente amenazas emergentes que pongan en vilo su normal desarrollo o incluso que sean instrumentalizados por la IA de manera inadecuada.

Por tanto, la protección y gobernanza de datos que promueve el CONPES es una medida que busca la seguridad digital en la sociedad, pues el dato es diseñado como el núcleo básico de toda estructura digital, que puede ser explotado por actores malintencionados e incluso a través de la IA que potencializa su margen operativo.

A su vez el eje de prevención y mitigación de riesgos adquiere relevancia para blindar el ecosistema de la IA frente amenazas digitales, entre ellas el TDig.

La relación existente entre la disponibilidad y gobernanza de los datos y el eje de prevención y mitigación de riesgos del CONPES 4144 del 2025 es intensa, por cuanto ambos ejes se enriquecen y suman su trabajo formando un sólo y común objetivo, el de fundamentar y basar el desarrollo de la inteligencia artificial en Colombia, en seguridad, en ética y en protección de la información.

Ciertamente los datos constituyen el principal insumo para el entrenamiento y mejora de los sistemas de IA; pero al mismo tiempo, representan un bien susceptible de ser vulnerado por riesgos inherentes al Ciberespacio, el TDig y la cibercriminalidad

Así pues, la gestión de datos junto con la mitigación de los riesgos en la IA, confluyen en un mismo propósito: garantizar una infraestructura digital transparente, responsable y segura del país.

Logrando proteger la integridad del sistema informático, los derechos o libertades de la persona, frente a las amenazas del mundo digital; reafirmando, que el desarrollo tecnológico se debe sustentar con una cultura protectora y vigilante.

Bajo este referente, la relación entre la gobernanza de datos, la prevención de riesgos y la IA, que plantea el CONPES 4144 de 2025 debe ser analizado a la luz de la TDPE a fin de observar si, frente a las nuevas amenazas digitales como el TDig o el mal uso de la IA, adopta medidas más estrictas de control y protección.

Aplicación de Matriz: Pestaña No. 4 denominada “Aplicación CONPES 4144 de 2025” https://docs.google.com/spreadsheets/d/1iOI6dUN6RR9xWH8HnKCkNVDx_oiGXptHM8rkKq75NhI/edit?usp=drive_link

Análisis.

Desarrollando la matriz, se identifica que el CONPES 4144 de 2025 va más allá de una hoja de ruta. Bajo la aplicación, de los fundamentos teóricos del TDPE se obtuvo un promedio

general de 1.875 (menor al anterior CONPES), advirtiendo que el documento presenta una aplicación parcial con tendencia funcionalista conforme a la escala establecida.

En otros términos, el documento no materializa de manera integral los postulados de esta teoría, sino que incorpora algunos de sus principios adaptados al ámbito tecnológico; en lo relativo a la forma en cómo se considera: la prevención, la vigilancia y la gestión del riesgo social desde la IA.

El CONPES 4144 no es un texto jurídico punitivo, es una política pública enfocada en el desarrollo tecnológico propiamente en la inteligencia artificial. No obstante, su discurso y su propia estructura revelan una racionalidad funcionalista.

El Estado se constituye en garante del orden y de la estabilidad del sistema y, la IA actúa como el instrumento que anticipa, neutraliza y gestiona los riesgos. Este enfoque preventivo y predictivo guarda afinidad con el funcionalismo sistémico de Jakobs, en tanto que prioriza la estabilidad del sistema sobre la autonomía individual

Ahora bien, se identifica que el Derecho Penal del Enemigo (DPE), se centra primordialmente en la prevención y el control de sujetos peligrosos, pero esta política trasladó su lógica a una guiada por una gobernanza digital del riesgo y previsión, en la que el ciudadano, a través de la IA, contribuye y es protegido por el sistema frente a diversas amenazas.

Por consiguiente, la IA se convierte en una herramienta que potencia el sistema, pero a su vez es un instrumento de control, predicción y observación al servicio del poder.

Continuando con este razonamiento, se tiene que el modelo planteado por el CONPES es eminentemente preventivo y anticipatorio, se dirige a la detección de riesgos futuros mediante instrumentos predictivos, supuestos y alarmas de detección temprana desarrollado por el Estado, el cual ya no contempla los hechos concretos consumados, sino que incluso actúa sobre probabilidades de ocurrencia por IA, consolidando un modelo de control ex ante.

Esta técnica se presenta como un medio para proteger derechos y la seguridad, pero a la vez instiga la construcción de una cultura de vigilancia permanente, donde el prevenir se relaciona con las libertades.

Por otro lado, el CONPES 4144, adopta una definición de ética con implicación de carácter jurídico, de la siguiente manera:

En alineación con la Recomendación sobre la Ética de la IA desarrollada por Unesco y adoptada por Colombia en 2022, para efectos del presente documento, el concepto de ética se entenderá como una reflexión normativa sistemática, basada en un marco integral, global, multicultural y evolutivo de valores, principios y acciones interdependientes.

Lo anterior, puede guiar a las sociedades a la hora de afrontar de manera responsable los efectos conocidos y desconocidos de las tecnologías de la IA en los seres humanos, las sociedades, el medio ambiente y los ecosistemas y les ofrece una base para aceptar o rechazar las tecnologías de la IA**(**Consejo Nacional de Política Económica y Social, 2025, p.39).

Esta definición es fundamental en tanto, convierte la ética en un punto de referencia normativo institucionalizado. Aunque intenta impulsar un uso responsable de la IA también puede funcionar como una herramienta para evaluar y/o controlar moralmente el comportamiento de los actores digitales al determinar quien actúa de manera correcta dentro del sistema y quién no.

Teniendo en cuenta este criterio, implícitamente, el documento realiza una distinción entre “actores éticos” y aquellos “actores no éticos”, lo cual conlleva a una nueva exclusión: personas que cumplen principios éticos del uso responsable de la IA (conforman la pertenencia al sistema) y quienes no cumplen (constituyen el riesgo del sistema).

> Esta clasificación moral no llega a convertir al “actor no ético” en un actor peligroso, ni en una sanción penal, pero sí existe la vigilancia de la conducta mediante controles, el seguimiento y la verificación constante donde la "ética" es utilizada como una forma de regular la conducta. En otras palabras, el “actor no ético” acaba sustituyendo al actor peligroso y la sanción penal es sustituida por la vigilancia previa y la evaluación moral.

De igual manera, si bien esta política pública se encauza en el ámbito administrativo, toca de manera leve la criminalidad al instruir al Ministerio de Defensa para emplear inteligencia artificial en la identificación de actividades ilegales asociadas al multicrimen de la siguiente manera:

> El Ministerio de Defensa Nacional, con el apoyo del Ministerio de Tecnologías de la Información y las Comunicaciones, desarrollará y ejecutará espacios de creación colectiva dirigidos a jóvenes sobre el uso de la inteligencia artificial para identificar actividades ilegales asociadas al multicrimen, que permita fortalecer las capacidades de investigación, desarrollo e innovación tecnológica del sector Defensa, en el marco del funcionamiento del Hub Fuerza Innovación. Esta acción iniciará en 2025 y finalizará en 2026 (Consejo Nacional de Política Económica y Social, 2025, p. 103)

A simple vista, el pasaje parece propugnar por formación ciudadana, educativa al involucrar al estatuto juvenil en proyectos tecnológicos con fines de innovación. Sin embargo, el hecho de que se inscriba en un apartado de seguridad y defensa, la directriz adquiere otro matiz.

Aquí los jóvenes no tienen un papel de receptores pasivos de la información, sino de promotores incipientes de la vigilancia. El Estado los forma en el uso de la IA para detectar actividades delictivas, lo que descentraliza el control y distribuye la función de observación social entre la ciudadanía.

En términos de Foucault (2007), se trata de una gubernamentalidad preventiva, donde el poder ya no se ejerce sólo desde arriba (el Estado), sino que se distribuye entre los sujetos, que comienzan a vigilar, analizar y controlar en nombre de la seguridad colectiva, agregando un ingrediente la inteligencia artificial.

Los jóvenes son el vector de expansión del control algorítmico; es decir, aprenden a usar la IA no solo para innovar, sino para mantener el orden social; por ello, la IA deja de ser una herramienta técnica o pedagógica para convertirse en un dispositivo de control penal preventivo.

También se advierte, una amenaza de deshumanización del individuo; en vista de que el sujeto al ser tratado como proveedor de datos y unidad de riesgo dentro del sistema puede transformarse en un componente dentro del ecosistema algorítmico, susceptible de ser observado, clasificado y gestionado según criterios de riesgo, eficiencia o vulnerabilidad pro la inteligencia artificial.

Por último, esta política también estimula la aplicación de la IA en contextos de excepcionalidad como el de la seguridad nacional, el de los desastres naturales o el de la protección de poblaciones vulnerables. En estos casos, el Estado se esfuerza por la intensificación de la vigilancia y el control de la forma de legitimar una "excepcionalidad tecnológica permanente", donde la intervención es normalizada ante la condición del riesgo, que permanece.

En resumen, el CONPES 4144 de 2025 evidencia una aplicación parcial de la TDPE, reinterpretada desde una lógica tecnológica. Su racionalidad funcionalista antepone la pervivencia del sistema a la autonomía del sujeto y su discurso ético oculta una estructura de control y vigilancia.

El índice de 1.875 vuelve a evidenciar que no hay aplicación del modelo de Jakobs, pero sí existe una tendencia generalizada hacia la prevención, la neutralización y la anticipación del control del comportamiento social.

Bajo el paraguas de la confianza digital y la seguridad el Estado desplaza la idea de justicia por la idea de administración del riesgo, convirtiendo a la IA en el nuevo instrumento de regulación del orden social. De forma que el ciudadano ya no es protegido como sujeto de derechos sino observado como una mera amenaza potencial, dentro de un paradigma en el que la prevención reemplaza al derecho y donde la eficiencia técnica se impone sobre la libertad.

- Consideraciones Finales.

Durante el periodo comprendido entre 2020 a 2025, el desarrollo de la política pública del Estado colombiano en el Ciberespacio, reflejada en los CONPES 3995 del año 2020 y el CONPES 4144 del año 2025, revela un cambio de paradigma sobre la concepción de la seguridad a nivel digital.

El énfasis, recae en el desplazamiento de una política ciberseguridad técnica hacia una política de seguridad digital cuyo eje es la gestión del riesgo que se cimenta sobre la prevención y cooperación institucional e internacional desde las tecnologías.

A partir de los documentos referenciados, se advierte una tendencia funcionalista del Estado, donde prima la estabilidad del sistema digital por encima de la autonomía personal, reproduciendo parcialmente la lógica preventiva y neutralizadora, propia de la Teoría del Derecho Penal del Enemigo (TDPE).

En efecto, la aplicación de la matriz en el CONPES 3995 del año 2020, con un promedio de 2,125, evidencia una implementación parcial, pues, aunque esta política en la actualidad orienta la implementación de la seguridad digital, se enmarca desde un espectro político-administrativo no penal.

No obstante, a pesar de ello, se observa una distinción práctica entre actores confiables versus riesgos o amenazas, dentro de un sistema de vigilancia administrativa que busca la neutralización preventiva en aras de dar continuidad y estabilidad al orden social en el ámbito digital.

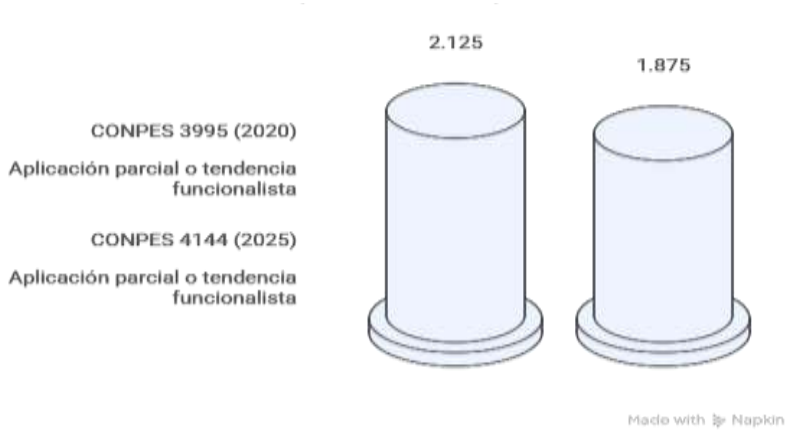
Desde esta perspectiva, esta categoría funcionalista es trasladada al CONPES 4144 de 2025, terreno del uso responsable de la inteligencia artificial (IA), que sin abocar a medios de control punitivo gesta una política de vigilancia anticipada donde la IA acta como herramienta de prevención, detección y neutralización para mantener el sistema social.

Como resultado, la matriz arrojó un promedio de 1.875, reiterando la aplicación parcial de TDPE, con un grado de funcionalismo desde la gobernanza del algoritmo del riesgo.

Así las cosas, se tiene lo siguiente:

Figura 31.

Promedio de aplicación de TDPE por CONPES (2020–2025)



Fuente: Elaboración propia en Napkin resultados de Matriz (2025).

En esencia, los dos CONPES construyen una lógica funcionalista sistémica en el que el ciudadano pierde protagonismo y es integrado como componente del sistema tecno-administrativo, cuya meta principal, no es la garantía de derechos, sino mantener y afianzar la estabilidad digital del país.

Es así como, las políticas públicas hacen constar un cambio en el paradigma de la seguridad digital: del énfasis técnico en las infraestructuras a la gobernanza moral y algorítmica del comportamiento social; considerando que ambas formas subrayan que el riesgo debe ser anticipado y gestionado antes que, combatido, constituyendo la prevención como principio orientador de la acción del Estado.

Esta mutación, aunque inspirada por la voluntad de proteger el espacio digital, genera una zona de conflicto con los principios garantistas del Estado Social de Derecho (ESD), pues permite que la vigilancia y el control sean condiciones permanentes de la gobernanza por debajo de cuerda.

Por otro lado, otro punto en común es que los documentos consideran el TDig de manera indirecta; en primer lugar, el CONPES 3995 de 2020 establece la amenaza digital como cualquier acción capaz de alterar la integridad de la información o la estabilidad de las infraestructuras y, aunque no tipifica el TDig, sí deja abierta la posibilidad de entenderlo en su condición de riesgo inminente y global.

En segundo lugar, el CONPES 4144, en cambio, se establece un marco más amplio porque establece una conexión entre IA, prevención de actividades delictivas y protección de datos estratégicos, aportando cierto sentido de un modelo de vigilancia preventiva y una resiliencia digital frente a posibles actos de desestabilización tecnológica.

Ambos, por tanto, ayudan a elaborar una doctrina estatal de anticipación del TDig, que funciona más como gestión y coordinación que como represión o penalización.

De esta comparación, se concluye que la hipótesis inicial del estudio, consistente en afirmar que el TDig en Colombia, particularmente en el período comprendido entre 2020 a 2025, en Colombia no ha evidenciado una tendencia hacia la incorporación de rasgos de la TDPE de Günter Jakobs.

Observable en el fortalecimiento de las sanciones, la creación de nuevos tipos penales y la flexibilización de garantías procesales frente a conductas cibernéticas consideradas amenazas al Estado resulta ser errónea ya que ninguno de los documentos establece un endurecimiento penal, ni existe un traslado directo de los postulados de Jakobs al ordenamiento jurídico colombiano. Entre.

Finalmente, la interrelación de ambos CONPES, despliega cómo la noción de enemigo se disuelve en la figura del riesgo en tanto que el TDig queda subsumido en un fenómeno administrable más que punible.

El Estado no castiga al enemigo en el TDig dado a atipicidad, sino que lo previene, lo controla y lo regula. De ahí que Colombia no asuma el Derecho Penal del Enemigo (DPE), pero sí retenga su lógica anticipatoria, en ese nuevo modelo de gobernabilidad digital.

En consecuencia, se obtiene un modelo híbrido en cuyo seno la seguridad asume el rol de valor supremo, la prevención es su manera de actuar y la tecnología —ya sustentada en la inteligencia artificial— de instrumento de su legitimidad.

Sin embargo, esta tendencia global plantea interrogantes sobre su compatibilidad con los principios garantistas y humanistas del Estado Social de Derecho (ESD), especialmente en contextos donde la expansión tecnológica redefine las fronteras del ius puniendi.

2.4. Capítulo IV. Terrorismo Digital en Colombia: una visión crítica desde el Estado Social de Derecho.

Entre 2020 a 2025, en lo referente al fenómeno del TDig la respuesta del Estado Colombiano; a pesar de constituir una amenaza latente acelerada por la pandemia COVID-19, aún carece de una regulación específica dentro del marco del Derecho Penal que sigue anclado a la realidad material y no a las nuevas dinámicas del Ciberespacio.

Por el contrario, se suscita que ante los hallazgos encontrados-en aplicabilidad de la matriz-frente a políticas públicas tendiente a establecer la seguridad digital en Colombia no se adopta un modelo punitivo de exclusión como lo es la TDPE, pero si privilegia una racionalidad de gestión del riesgo y prevención sistémica.

En este contexto, resulta indispensable volver sobre el estándar constitucional que orienta la actuación estatal, esto es, el Estado Social de Derecho (ESD), el cual define el alcance legítimo del *ius puniendi* en entornos digitales y la política pública de la misma.

2.4.1. El Estado Social de Derecho: fundamento constitucional y principios rectores.

El primer artículo de la Constitución Política de Colombia (1991) consagra de manera taxativa la forma de organización del Estado, amparado bajo un Estado Social de Derecho (ESD) que reconoce la dignidad humana, el trabajo, la solidaridad y la prevalencia del interés general como pilares esenciales de su orden político y jurídico (Colombia. Asamblea Nacional Constituyente, 1991, art. 1).

Bajo esta fórmula, se consolida la identidad jurídica, filosófica y política del Estado colombiano, lo cual, significó un cambio de paradigma entre la relación Estado/Particular al consolidar desde una visión antropocentrista el Estado al servicio del ser humano.

Históricamente, con la Constitución de 1886, Colombia adoptó una organización basada en el modelo de Estado de Derecho, caracterizado por la supremacía de la ley o también denominado "gobierno de las leyes", donde la persona se subordina al marco normativo, por encima de sus garantías fundamentales.

Sin embargo, contempla los doctrinantes William Bermúdez y Juan Carlos Morales (2012) que "los cambios político-sociales generados a nivel mundial, los cambios de paradigma normativos, la concepción del derecho para regular las relaciones sociales de las personas en su cotidianidad, produjo que se gestaran en Colombia nuevas instituciones jurídico-políticas" (p.65) entre ellas la Constitución de 1991, adoptando un modelo de Estado Social de Derecho (ESD).

Con esto en mente, bajo esta cláusula fundacional se consolidó el Estado Social de Derecho (ESD) en Colombia, materializando una ruptura del modelo tradicional y encaminado a equilibrar el respeto de la norma con la justicia social; en tanto, su visión se centra en la satisfacción de necesidades materiales del ser humano propias de su existencia.

De allí que, se pueda aseverar que "la idea de lo "humano" invade el concepto de Estado Social de Derecho (ESD), mientras que la noción "hombre" lo hace frente al Estado de Derecho" (Cabrera, 2018, p. 5).

En verbigracia, el Estado Social de Derecho, desde ahora ESD, reformulo los sistemas sociales, políticos y económicos del país, con el objetivo de garantizar el bienestar de los individuos en la sociedad.

En este sentido, este nuevo modelo implica una participación activa del Estado frente a la praxis social, en aras de corregir desigualdades del sistema, así como garantizar la efectividad de los principios, derechos y deberes fundamentales que provee la constitución de 1991, la cual ha de ser interpretada a través de la óptica de estos preceptos.

Según la Corte Constitucional en Sentencia T-421 de 2017, establece que "El principal objetivo del Estado Social de Derecho es garantizar la eficacia de los derechos. Por consiguiente, no se puede dar prevalencia a los procedimientos, ni al instrumento procesal, sobre el derecho sustancial" (Corte Constitucional, 2017b, M.P. Iván Humberto Escruceria Mayolo).

En coadyuvancia, en Sentencia C-566 de 1995, la Corte Constitucional estableció que el propósito principal del ESD "es procurar las condiciones materiales generales para lograr su efectividad y la adecuada integración social. A la luz de esta finalidad, no puede reducirse el Estado Social de Derecho a mera instancia prodigadora"(Corte Constitucional, 1995d, M.P. Eduardo Cifuentes Muñoz).

Así las cosas, la jurisprudencia constitucional ha determinado que el ESD no puede suprimir su esencia a un aparato benefactor, debe orientarse a garantizar la efectividad de derechos a través de la creación de condiciones materiales y sociales que hagan posible la realización efectiva de todas las personas en sociedad.

En esta misma línea, la Corte Constitucional en sentencia C-1064 de 2001, determinó que el Estado Social de Derecho (ESD), como forma de organización estatal debe orientarse a garantizar dos categorías: justicia social y dignidad humana, concretado por la institucionalidad. (Corte Constitucional, 2001b, M.P. Manuel José Cepeda Espinosa y Jaime Córdoba Triviño)

La Corte resaltó en este pronunciamiento la necesidad de promover una relación dinámica entre Estado/Sociedad, encaminada a la consecución de condiciones reales de libertades individuales, pero también que se pongan en movimiento para contrarrestar las desigualdades sociales existentes (Bermúdez & Morales, 2012).

Por ende, el ESD, se interpreta a través de la óptica de los derechos fundamentales como un instrumento creado para facilitar la convivencia a partir de estos, donde el Estado adquiere un papel activo en protegerlos.

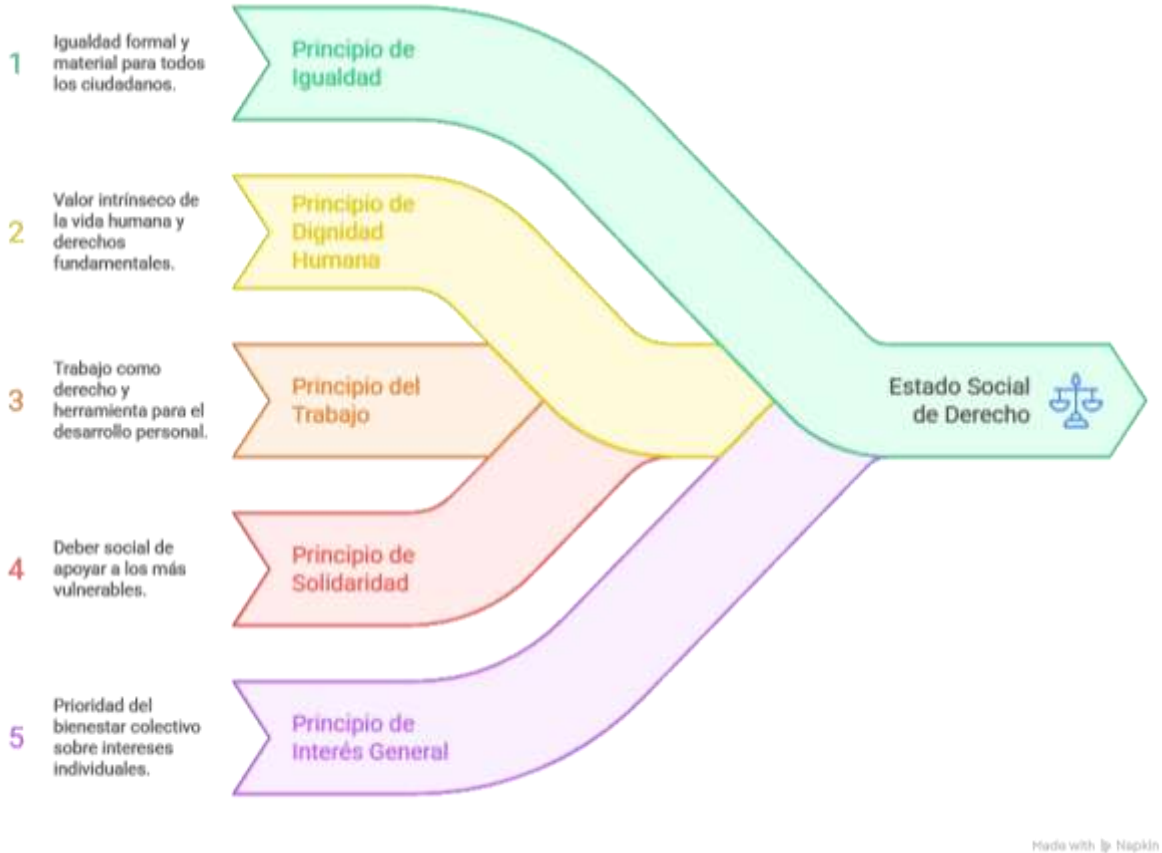
En virtud de lo anterior, se crea un sistema cada vez más completo de garantías que se centra en la protección del ser humano atendiendo a sus condiciones reales al interior de la sociedad

y no del individuo abstracto; que hace cierta y eficaz la responsabilidad del poder público frente a posibles vulneraciones.

En este contexto, Colombia siendo un ESD se fundamenta en cuatros principios esenciales que orientan la acción estatal y a su vez constituyen los cimientos ético-jurídicos que representan la relación entre Estado/Particular; pues a través de ellos se delimita y orienta el poder público, garantizando la protección de los derechos fundamentales y la realización del bien común, los cuales son:

Figura 32.

Principios Constitucionales del Estado Social de Derecho (ESD).



Fuente: Elaboración propia en Napkin con base en (Bermúdez & Morales, 2012)

El constituyente originario dio la más alta fuerza normativa a una concepción ética del ejercicio del poder, según la cual, nada está por encima del respeto y garantía de los derechos humanos y principios constitucionales, ni siquiera en los Estados de excepción.

En coherencia con este mandato, Colombia siendo un ESD está fundado en el respeto de la dignidad humana, el trabajo, la solidaridad de las personas que la integran y en la prevalencia del interés general, establecidos en el artículo 1°; en conjunto con la igualdad material, como eje transversal (Colombia. Asamblea Nacional Constituyente, 1991, art. 1).

Ahora bien, al establecer la constitución un ESD fundado la dignidad humana, no solo la erigió como valor fundante, también como derecho, finalidad y principio constitucional que-desde una concepción kantiana-refiere el valor intrínseco de la vida humana, como fin en sí mismo y no como medio.

De allí que, este principio sea considerado superior a todos los demás y presente características de ser absoluto, hasta el punto de ser presentado como el fundamento de los demás principios y derechos fundamentales (Mendieta y Tobón, 2018)

Según el Tribunal constitucional en sentencia T-1096 de 2004 (M.P. Manuel José Cepeda Espinosa) su protección dentro de un ESD se impone en 3 ámbitos a saber: en primer lugar la autonomía personal y autodeterminación en su proyecto de vida (vivir como quiera); en segundo lugar como garantía de condiciones materiales para una adecuada existencia (vivir bien).

Por último, como la inviolabilidad de la integridad tanto física como moral, que impide el trato degradante (vivir sin humillaciones).

Estos preceptos no parten de un referente natural, por el contrario, son contenidos concretos en los cuales el ser humano se desarrolla en comunidad, por lo que, dentro del sistema, la dignidad humana es el criterio articulador; “el presupuesto esencial de la consagración y efectividad del entero sistema de derechos y garantías contemplado en la Constitución” (Corte Constitucional, . 1992a, Sentencia T-401 de 1992, M.P.: Eduardo Cifuentes Muñoz)

De esta manera, el ESD al dirigir su estructura a atender al ser humano, encuentra en la dignidad humana criterio operativo para que toda persona pueda vivir con autonomía, bienestar y respeto.

En cuanto, al principio de igualdad, el ESD se aleja de la mirada clásica-liberal de la igualdad formal, si bien el artículo 13 constitucional, traes a colación la premisa de que todos los individuos son libres e iguales y poseen un trato indistinto ante la ley; el segundo y tercer párrafo del articulado materializa el fin de la institución propia de esta forma de organización estatal al desglosar la igualdad material.

La igualdad material, parte del reconocimiento de la existencia de desigualdades que despliega el sistema social, los cuales constituyen un obstáculo para gozar de una vida "digna" y consecutivamente de ejercer derechos fundamentales, de allí, la búsqueda del Estado por buscar un mejor acceso.

Su contenido no se limita a una directriz, requiere la implementación de garantías plenas; sobre este aspecto Ara Pinilla (2000) dispone:

> (...)la igualdad en los derechos puede significar no sólo que todos los hombres seamos igualmente titulares de derechos ni que todos podamos ejercitar en igual medida nuestros derechos, sino también, si se admite como derecho la expectativa de todo ser humano a equipararse en la tenencia de bienes y aptitudes con sus semejantes (p.205).

Ello supone, que este principio debe permitir a las personas el acceso de manera conjunta y en las condiciones equitativas a todos los bienes materiales y oportunidades necesarios para el desarrollo de su existencia (vivir bien) una meta a perseguir en una estructura económica capitalista. De allí, que surjan las acciones afirmativas para proteger a sectores vulnerables.

En consecuencia, el Estado se configura genéticamente para servir como instrumento a la garantía y realización de los derechos que se desarrolla en el marco del principio de igualdad para suprimir las discrepancias sociales.

Por otro lado, el principio de trabajo, se erige como una realización del individuo a nivel personal y colectivo, por lo que adquiere un carácter de derecho fundamental (art. 25-53), principio y deber social que dignifica a la persona para la consecución de sus necesidades y contribuye al mantenimiento del orden al participar activamente en un rol social.

La figura del ESD en este principio es que "expone y justifica la intervención del Estado en la economía, dignificando al ciudadano colombiano con empleo y permitiendo su acceso efectivo a los bienes y servicios básicos" (Bermúdez & Morales, 2012, p. 68).

El principio de solidaridad desarrollado en el artículo 1° y 95 núm. 2 de la constitución es "un deber, impuesto a toda persona por el solo hecho de su pertenencia al conglomerado social, consistente en la vinculación del propio esfuerzo y actividad en beneficio o apoyo de otros asociados o en interés colectivo" (Corte Constitucional, 2014, Sentencia C-767 de 2014, M.P.: Jorge Ignacio Pretelt Chaljub).

En consecuencia, la solidaridad es un principio que mantiene en firme el pacto social, al traducirse en la corresponsabilidad que tienen todos los miembros con sus semejantes y con la sociedad.

La jurisprudencia constitucional ha manifestado que existe para los individuos una obligación para ayudar a sus "congéneres" para hacer efectivo no solo los derechos del individuo sino del otro. (Corte Constitucional, 2014, Sentencia C-767 de 2014, M.P.: Jorge Ignacio Pretelt Chaljub).

Existe pues una construcción del bien común, un instrumento de cohesión social dentro del ESD, en la que el individuo está delimitado por su colectivo y debe prestar apoyo en comunidad.

Para finalizar, el principio de prevalencia del interés general, es una cláusula abstracta que debe ser optimizada en cada caso en particular, el ESD orienta su actuación hacia la búsqueda del bien común, no hacia intereses particulares, por lo que se convierte en un criterio para el desarrollo de políticas públicas y directrices del Estado.

Por último, los principios que permiten materializar el ESD, son una pauta de interpretación obligatoria dotada de plena fuerza normativa constitucional, que orientan la interpretación y aplicación de todo el ordenamiento jurídico.

La Corte Constitucional ha expresado en Sentencia T-406 de 1992, que estos principios son pautas inexcusables de interpretación y de actuación estatal, sin dejar de mencionar que su textura abierta obliga ponderaciones particularmente en cada caso específico (Corte Constitucional, 1992b, M.P. Ciro Angarita Barón).

Según Alexy (2004) expone, los principios se aplican, por lo demás, no como mera subsunción, sino mediante un ejercicio de optimización y equilibrio ante otros principios concurrentes.

Así, el Estado Social de Derecho (ESD) no es solo un marco formalista de legalidad, sino que actúa como un modelo dinámico que persigue la realización progresiva de la justicia material, como de la dignidad humana y de la efectividad de los derechos fundamentales. Asegurando, que la Constitución se encuentre viva en la práctica jurídica cotidiana.

Desde la óptica del ESD, la política pública constituye un instrumento para materializar los principios y valores de carácter constitucional que legitiman la acción pública. En esta visión, el Estado no solo es garante del orden, sino que se convierte en impulsor activo del bienestar colectivo y del desarrollo humano integral.

Por lo tanto, toda política pública, incluso en el ámbito de la seguridad o la tecnología, tiene que impulsar la cohesión social y la confianza en las instituciones, percatándose de que las respuestas no pueden ser solo coactivas o tecnocráticas, sino que las políticas en el ámbito de lo digital deben reflejar el principio de la preminencia de los derechos fundamentales que es el imperativo ético-jurídico del Estado Social de Derecho (ESD).

2.4.2. El Derecho Penal en el Estado Social de Derecho (ESD).

La supremacía constitucional, ha derivado en la constitucionalización del derecho, en especial, del Derecho Penal, en vista de que el Ius Puniendi del Estado, queda supeditado a los parámetros (valores, principios, derechos) constitucionales. La Corte Constitucional en sentencia C-038 de 1995 ha dispuesto:

> Ha habido una constitucionalización del Derecho Penal porque tanto en materia sustantiva como procedimental, la Carta incorpora preceptos y enuncia valores y postulados- particularmente en el campo de los derechos fundamentales- que inciden de manera significativa en el Derecho Penal y, a la vez, orientan y determinan su alcance (Corte Constitucional, 1995b, M.P. Alejandro Martínez Caballero).

Bajo este referente, el Derecho Penal se convierte en un instrumento de protección de bienes jurídicos, guiado por los principios de la carta constitucional, en especial por la dignidad humana, desplazando la relación de Estado/Particular, donde el primero sirve al último dentro del marco punitivo.

En su momento, Juan Fernández Carrasquilla (2006) manifestaba que la dogmática penal debía incorporar una reflexión valorativa o axiológica, teniendo en cuenta los principios superiores del orden constitucional; de modo que, la norma penal no solo contemple una validez formal dentro del sistema jurídico, sino adquiera una legitimidad a través de los valores axiológicos que sustenta el ESD.

En esta misma línea Ferrajoli (2001) sostiene que el Derecho Penal solo puede ser considerado como legítimo si se encuentra " algún sistema de garantías que protegen frente al poder del Estado"(p.25)

En consecuencia, el Derecho Penal ya no es un instrumento de control social, sino un instrumento encaminado a proteger garantías fundamentales.

Este cambio de paradigma, traduce en la necesidad de someter el ejercicio del ius puniendi a límites racionales y constitucionales para que las penas sean justificadas de conformidad con los valores superiores del ordenamiento, en especial la dignidad humana.

Lo anterior, por cuanto su ejercicio comporta una serie de restricciones frente a derechos fundamentales, como la libertad que no pueden quedar bajo márgenes de discrecionalidad al momento de imponer sanciones.

En sentencia C-936 del 2010, la Corte Constitucional (2010b, M.P. Luis Ernesto Vargas Silva) determinó que el ius puniendi "debe estar orientado a hacer efectivos esos derechos y valores constitucionales" de allí que su legitimidad derive de la sujeción del marco constitucional que sustenta el ESD, por lo que es un poder limitado.

Continuando con este razonamiento, la función el Derecho Penal no se enfoca en la retribución sino en la eventual protección del ser humano frente a posibles abusos del ius puniendi. Así, su desarrollo no radica en la severidad con que actúa sino en la moderación que le imponen los límites constitucionales.

De ello se desprende, que el Derecho Penal debe ser concebido como último recurso frente a conductas que lesionan gravemente los bienes jurídicos más importantes, de lo que deviene que debe reducirse en lo estrictamente necesario para proteger los derechos fundamentales.

En otras palabras, solo se activa cuando se observe conductas que sean una posible o efectiva lesión de bienes jurídicos colectivos o ante riesgos intrínsecos que impacten directamente los propios valores del Estado Social de Derecho (ESD).

La Corte Constitucional (2012) en Sentencia C- 365 de 2012 ha manifestado:

> El Derecho Penal se enmarca en el principio de mínima intervención, según el cual, el ejercicio de la facultad sancionatoria criminal debe operar cuando las demás alternativas de control han fallado. Esta preceptiva significa que el Estado no está obligado a sancionar

> penalmente todas las conductas antisociales, pero tampoco puede tipificar las que no ofrecen un verdadero riesgo para los intereses de la comunidad o de los individuos (M.P.: Jorge Ignacio Pretelt Chaljub).

Dentro de este marco, la intervención del Derecho Penal en sociedad es mínima, Ferrajoli (2001) sustenta que solo es admisible solo cuanto otros mecanismos han sido agotados, por lo que solo debe activarse en los casos estrictamente necesarios y no como instrumento genérico de control social o moral.

Según la Corte Constitucional (2019b), en sentencia C-233 de 2019:

> (…) la disponibilidad de otros mecanismos jurídicos para prevenir o combatir una determinada problemática social, económica, política o cultural, descarta y desplaza automáticamente la vía penal y que, por consiguiente, siempre que el Estado pueda enfrentar cierto fenómeno o práctica socialmente nociva mediante otras herramientas extrapenales, tiene vedado el camino criminal (M.P.: Luis Guillermo Guerrero Pérez).

La visión del Tribunal constitucional, contribuye a racionalizar, limitar y minimizar la función punitiva del Estado Social de Derecho (ESD), lo que deriva en la expresión misma del garantismo penal que corresponde a "la noción de un Derecho Penal mínimo, que intenta poner fuertes y rígidos límites a la actuación del poder punitivo del Estado" (Ferrajoli, 2006, p.7). Ferrajoli resume esta idea en el principio: No hay ley penal sin necesidad.

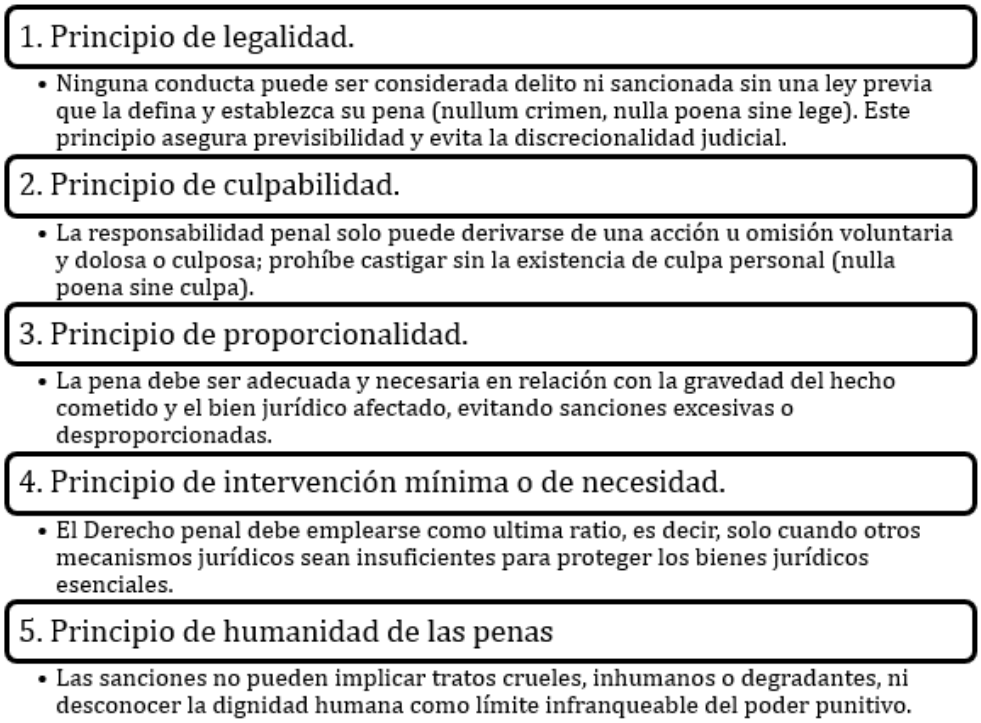
En este perspectiva el garantismo busca proteger al débil de la relación Estado/Particular, para que no le sean vulneradas de manera sistema sus garantías, pues este no busca fortalecer la capacidad del Estado para castigar, sino para imponer límites a fin de evitar arbitrariedades. "El Derecho Penal debe concebirse como un sistema de garantías en defensa de los derechos del ciudadano frente al poder punitivo del Estado"(Ferrajoli, 1995, p. 28).

Con esto en mente y una vez sustanciado el principio de intervención mínima como eje de la teoría a del garantismo penal, es preciso subrayar que no es el único límite posible al ius puniendi del Estado; junto a él, el Derecho Penal contemporáneo viene reconociendo otros

principios que persiguen tanto racionalizar como limitar el ejercicio del poder punitivo, garantizando así la protección efectiva de los derechos fundamentales. Estos son:

Figura 33.

Límites al Ius Puniendi según el Garantismo Penal.



Fuente: Elaboración propia con base en Ferrajoli, L. (1995).

Frente al *principio de legalidad*, el artículo 29 de la Constitución Política de manera taxativa establece "Nadie podrá ser juzgado sino conforme a leyes preexistentes", ello significa que no puede existir una sanción sin una ley previa, clara y escrita. Ferrajoli (2004) sintetiza este postulado con su célebre frase: *"*No hay delito ni pena sin ley previa, ni juicio sin prueba, ni prueba sin contradicción" (p. 78).

La Corte Constitucional bajo este mismo eje ha dispuesto en sentencia C-710 de 2001 (2001b, M.P.: Dr. Jaime Cordoba Triviño) que el principio de legalidad es un principio rector del ejercicio de poder dual: por un lado determina el uso de las facultades para legislar y la sanciones

que de ella de deriven. Sin embargo también, define “la relación entre el individuo y el Estado al prescribir que el uso del poder de coerción será legítimo solamente si está previamente autorizado por la ley”.

Ahora, con la constitucionalización del Derecho Penal, el principio de legalidad debe ser observado desde “firmes referentes materiales de valor encarnados en la persona humana, orientado por el principio pro-homine” (Cote, 2008, p.130).

Por su parte, el *principio de culpabilidad* deriva de la prohibición de sancionar a alguien sin demostrar su responsabilidad, una derivación del derecho a la presunción de inocencia; reconocido en el texto constitucional en el artículo 29 al disponer “Toda persona se presume inocente mientras no se la haya declarado judicialmente culpable” siendo necesario que la conducta endilgada sea obra del individuo al que se le imputa.

La Corte Suprema de Justicia en Sentencia SP-055 del 22 de Febrero de 2023 establece que este principio existe en un sentido amplio y estricto:

> En sentido amplio, implica que el individuo solo puede ser responsable por sus propios actos (personalidad de las penas). Así mismo, que únicamente puede responder por lo que hace o dejar de hacer, por sus conductas, no por lo que es, su personalidad o sus ideas (Derecho Penal de acto, no de autor (M.P.: Myriam Ávila Roldan, p. 9).

La Corte, encuentra este principio vinculado a la dignidad, a la vigencia de un orden justo y a la igualdad material pues asegura que el ius puniendi solo pueda fundarse en una conducta subjetiva, es decir sobre quien eligió voluntariamente infringir la norma. Ferrajoli, en *Derecho y razón. Teoría del garantismo penal* (1995), sostiene no hay pena sin culpabilidad.

El reproche que parte de la culpabilidad, en la cual, se espera que “la otra persona actuase de otra manera” debe ser relacionado de manera intrínseca al principio de la dignidad humana ya que, un ESD no puede exigir conductas que superen las posibilidades fácticas de sus ciudadanos; de modo que las condiciones sociales deben ser sopesadas al momento de juzgar (Cote, 2008)

Bajo el garantismo penal, más allá de las categorías dogmáticas y su constatación formal la imposición de la pena exige un la aplicación de principios constitucionales, entre ellos: la *proporcionalidad*, que como criterio de interpretación constitucional busca evitar el exceso punitivo y garantizar sanciones razonables y equilibradas; por lo que se convierte en un componente esencial para el Estado Social de Derecho (ESD) y para los derechos fundamentales.

De acuerdo a la Corte Constitucional en sentencia C-916 del 2002 es un postulado no explícito de la constitución de 1991, pero a pesar de ello "es un principio de corrección funcional de toda la actividad estatal que, junto con otros principios(…)busca asegurar que el poder público, actúe dentro del marco del estado de derecho, sin excederse en el ejercicio de sus funciones"(Corte Constitucional, 2002b, M.P.: Manuel Jose Cepeda Espinosa).

Para Ferrajoli (1995) "la pena sólo puede ser legítima en cuanto sea necesaria y proporcionada al daño causado y a la culpabilidad del autor" (p.340)

Por último, el principio de humanidad de las penas, disposición desarrollada en el artículo 12 de la Constitución Política que dispone "Nadie será sometido a desaparición forzada, a torturas ni a tratos o penas crueles, inhumanos o degradantes.".

Este principio se orienta a que a pesar de haber generado una conducta contraria a derecho y recibir una condena bajo un juicio justa, el Estado debe respetar la dignidad de la persona; en consecuencia, la penda no debe degradar, ni despojar al individuo de su condición de persona, sin o contribuir a su reinserción.

Ferrajoli (2004) complementa esta idea al afirmar que "la prisión sólo puede justificarse si respeta la humanidad del reo y tiende a su reintegración social"(p.213); en verbigracia la Corte Constitucional en sentencia C-108 de 2017 dispone:

> los límites constitucionales al ejercicio de la potestad punitiva del Estado pueden ser explícitos e implícitos. Como límites explícitos se han identificado la prohibición de la pena de muerte (art. 11); el no sometimiento a desaparición forzada, torturas, ni a tratos o penas crueles, inhumanas o degradantes (art. 12); la prohibición de las penas de destierro,

> prisión perpetua y confiscación (art. 34); entre otras. En cuanto a los límites implícitos, se ha destacado que el legislador penal debe propender por la realización de los fines esenciales del Estado como son los de garantizar la efectividad de los principios, derechos y deberes constitucionales y asegurar la convivencia pacífica y la vigencia de un orden justo (Corte Constitucional, 2017a, M.P.: Luis ErnestoVargas Silva)

Complementando dicha idea, la doctrinante Zeneida López (2001) establece que el Derecho Penal debe trascender sus fronteras positivistas y encaminarse a su constitucionalidad; cuyo pilar dogmático es la dignidad.

Si la mera dignidad no basta, se debe llegar al elemental principio de humanidad, para que funja como exigencia del respeto a los derechos humanos fundamentales, condición que en ninguna circunstancia puede desconocer al ser humano, pues aún bajo el estigma de haber delinquido, dentro del proceso penal, es sujeto y no objeto.

Es así como, el ius puniendi dentro del Estado Social de Derecho (ESD) colombiano, no es un poder en expansión, sino un poder constitucionalmente limitado en cuanto que la dignidad humana, la libertad y los principios de legalidad, culpabilidad, proporcionalidad y humanidad constituyen límites que transforman el castigo en una función buena y racional del ius puniendi que no se asemeja al despotismo.

Desde la teoría garantista de Ferrajoli, tales principios no van a quedar reducidos a simples normas de técnica jurídica, sino que van a describir auténticas garantías políticas y morales protectoras frente al Estado.

Las anteriores consideraciones, permiten afirmar que el único Derecho Penal que es permitido por el Estado Social de Derecho (ESD), desde el funcionalismo, es el funcionalismo teleológico de Claus Roxin.

Como se ha mencionado en capítulos anteriores, Roxin, en su obra “Política criminal y sistema del Derecho Penal” (1963), sostiene que el Derecho Penal no debe analizarse siempre desde una estructura dogmática, sino desde la función que cumple dentro de la sociedad, para ello

se enfoca en los fines político-criminales del Estado de Derecho, unificando tres ámbitos: política criminal, dogmática penal y fines de la pena; logrando así un funcionalismo teleológico.

A la luz de lo anterior, el marco dogmático que ofrece la teoría del funcionalismo teleológico de Claus Roxin resulta plenamente acorde con los valores del Estado Social de Derecho (ESD), pues la función y finalidad del Derecho Penal no puede entenderse de manera formal o aislada de la realidad social.

Por el contrario, debe ser entendido como un instrumento puesto al servicio de la comunidad, lo que aproxima a esta disciplina a una noción de justicia social definitiva entendida como el cuidado de los bienes jurídicos comunes, de la dignidad humana y de la protección de la libertad individual..

2.4.3. Pugna entre los principios del Estado Social de Derecho (ESD) y los fundamentos teóricos del Teoría del Derecho Penal del Enemigo.

El doctrinante Nodier Agudelo (2014) manifiesta que la dimensión punitiva del Derecho Penal cumple esencialmente un rol de control social, quien los ejercen se justifican en la necesidad de preservar valores fundamentales que sostienen la convivencia social, lo cual genera una evidente paradoja:

> (…) la libertad de los ciudadanos se limita a través de la norma y por ello el Derecho Penal es represión; sin embargo, la norma es también libertad en la medida que indica cuál es la órbita de actuación del Estado y su injerencia en el ciudadano, señalando que le queda de este (p.24)

De allí, se advierte que, la práctica contemporánea, contemplan dos esferas en pugna sobre la naturaleza del Derecho Penal (garantista/punitiva) pues su dilema gira en torno a una controversia histórica la libertad versus la seguridad.

Bajo esta perspectiva, es previsible que la visión garantista que contempla el Estado Social de Derecho (ESD) derive en un conflicto claro frente a los fundamentos de la TDPE de Gunter Jakobs.

La propuesta de Jakobs plantea dos derechos penales que coexisten en el desarrollo cotidiano del Estado: ciudadano y el del enemigo.

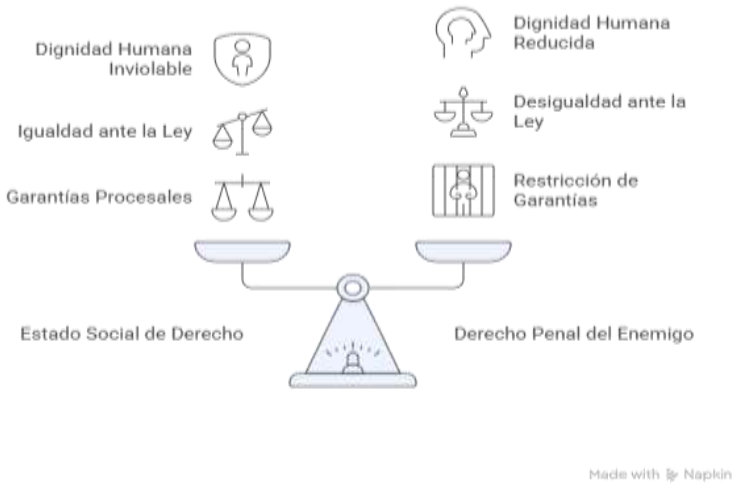
En cuanto al Derecho Penal del ciudadano, es una categoría de aplicación clásica donde el que infringe la norma sigue siendo tratado como persona, pues no ha quebrantado el pacto social o abandonado las reglas mínimas de convivencia, en consecuencia, solo basta la pena para reafirmar la norma frente a la sociedad.

En este Derecho Penal, se mantienen las garantías del Derecho Penal tradicional, no existe per se, algún fundamento en contrario que permita concluir lo contrario; por esta razón, en este sistema jurídico los principios del ESD se mantienen incólumes.

Ahora bien, no es posible afirmar lo mismo del Derecho Penal del Enemigo (DPE), propuesto como segunda categoría, frente aquellas-no personas- estos son: aquellos individuos que significan una amenaza permanente para el pacto social, pues no solo solo infringe las normas, sino que busca desaparecer la validez del sistema jurídico-político en su totalidad, siendo insuficiente el Derecho Penal del ciudadano para su tratamiento.

Figura 34.

Conflicto del ESD frente al TDPE.



Fuente: Elaboración propia en Napkin.

Para el ESD la creación de este sistema ya comporta una frontal contradicción con los principios estructurales y axiológicos que sostienen el orden jurídico, por al menos cuatro razonamientos que se pasan a considerar a continuación:

- Dicotomía Ciudadano-Enemigo: La Negación de la Dignidad Humana.

Es el principal punto de incompatibilidad, teniendo en cuenta que un ESD se funda en la dignidad humana como criterio articulador del sistema jurídico, al verse el principio restringido o incluso ponderado bajo un Derecho Penal de excepción, pierde la esencia del modelo constitucional que lo sostiene.

Sobre la base de “no persona”, la TDPE reduce al ser humano a un objeto de control o neutralización, lo cual comprende una violación flagrante, muy a pesar de que su despersonalización se circunscriba solamente al ámbito penal ya su sola existencia deriva en una concepción instrumental del individuo.

Esta despersonalización es irreconciliable con el núcleo del ESD pues reconoce dignidad, incluso al delincuente que vulnera de manera ostensible el pacto social.

Según Robert Spaemann (1989)

> Esa dignidad se fundamenta en el carácter personal del hombre. Pero la independencia de la persona depende de que a ningún hombre le corresponde juzgar si otro hombre posee o no los rasgos fundamentales de la personalidad. Los derechos humanos dependen del hecho de que nadie tiene la prerrogativa de definir el círculo de aquellos a quienes corresponden o dejan de corresponder (p.22).

Lo anterior significa, que los derechos se fundamentan por la condición inherente de ser humano, sin que resulte jurídicamente viables criterios adicionales que limiten dicho reconocimiento dado por su existencia natural, como lo quiere hacer ver el TDPE.

Advierte Luigi Ferrajoli (1995) no hay Derecho Penal sin ciudadano y no hay ciudadano sin derechos fundamentales.

- Funcionalismo sistémico vs Protección de Derechos Fundamentales.

El ESD, se funda en garantizar la efectividad de los principios, derechos y deberes fundamentales de la carta constitucional, por lo que el Derecho Penal se encuentra subordinado a estos preceptos y debe ir encaminado a la protección de bienes jurídicos que la sociedad estime necesarios proteger.

No obstante, el funcionalismo sistémico es diametralmente opuesto, su finalidad es poner en marcha las expectativas normativas y restablecer la confianza por parte de los actores en el sistema tras la "perturbación" que supuso en su momento el delito. La pena se convierte en acto comunicativo-simbólico de la vigencia de la norma.

El aislamiento de la realidad, que desarrolla esta teoría; así como su aparente neutralidad, es esencial para la crítica garantista desde el ESD, debido a que, tal neutralidad es, en los términos

de Eugenio Raúl Zaffaroni (2006), una ficción ideológica que encubre un programa político de control o exclusión.

De allí, que, lejos de ser una ciencia aséptica, el Derecho Penal es, finalmente, una forma de ejercicio del poder y, por tanto, siempre está cargado de contenido político y axiológico.

Sostener que el derecho puede aplicarse sin referencias a valores-sin tener presente la dignidad humana, la igualdad, la justicia- es, tal como avisa Ferrajoli (1995), negar la esencia misma del constitucionalismo es volver a un derecho de fuerza, no de razón

- Dicotomía Ciudadano-Enemigo: Violación al principio de igualdad.

El enfoque binario, que presenta la tesis del profesor Günther Jakobs, surge de una realidad social que se distingue exactamente entre el "ciudadano" y el "enemigo", quiebra el principio de igualdad ante la ley, uno de los fundamentos del ESD, pues impone medidas excepcionales y restricción de garantías procesales de manera arbitraria con base en un criterio de peligrosidad.

En esta línea, advierte Eugenio Raúl Zaffaroni (2006) qué tal forma de entender que la TDPE constituye una ruptura en el universalismo jurídico moderno ya que introduce una categoría de seres humanos no protegidos jurídicamente.

De esta manera, el derecho se convierte en un instrumento de discriminación política y social, pues quien reconoce derechos es la norma y esta a su vez lo hace conforme al comportamiento que el individuo despliegue, de lo contrario puede ser sometido o incluso mermar su dignidad humana.

Y esta desigualdad es diametralmente opuesta al sentido del constitucionalismo contemporáneo, para Ferrajoli (1995), la medida de la legitimidad del Derecho Penal está precisamente en que trata a todos los hombres como sujetos dotados de igual dignidad, a pesar de que algunos traicionen el ordenamiento jurídico.

- Afectación de derechos fundamentales en especial garantías procesales.

La idea del enemigo desde la concepción de -no persona- en el ámbito punitivo, consecuentemente conlleva a la restricción supresión de garantías procesales básicas (al encontrarse supeditado a la anticipación de la punibilidad y actitud peligrosa) entre las más sonadas: presunción de inocencia, esta es eliminada de manera inminente, en conjunto con la defensa y la proporcionalidad de la pena.

Eugenio Raúl Zaffaroni (2006) advierte que la TDPE no se aplica al hecho cometido, sino a la persona que el poder político define como peligrosa y esto, junto con la legitimación de la punición preventiva, da paso a un tratamiento del procesal diferenciado.

Este desplazamiento convierte el proceso penal -la garantía- en un medio de control y de neutralización, desnaturalizando y despreciando la función del Derecho Constitucional y dando paso a un Derecho Penal del autor, que no es ni puede ser paralelo ni conforme a la igualdad, a la dignidad humana, a los derechos fundamentales por la persona.

Como sostiene Luigi Ferrajoli (1995), las garantías procesales no son meros formalismos, sino las condiciones necesarias de la legitimidad del poder punitivo. Sin ellas, el Derecho se convierte en “pura violencia institucional”, en la medida que ya no castiga hechos probados, sino identidades sospechosas o peligrosidades presuntas.

Ahora, si se observan los límites del ius puniendi se tiene:

Tabla 8.

Límites del ius puniendi vs TDPE.

Limites al ius puniendi.	Afectación por el Derecho Penal del Enemigo (Jakobs)	Consecuencias en el Estado Social de Derecho
Legalidad	Se amplían los tipos penales hacia conductas de peligro o mera sospecha, con normas vagas y abiertas que anticipan la punición.	Se debilita la seguridad jurídica y se sustituye la previsibilidad de la ley por el castigo político. El Derecho deja de ser límite y se convierte en instrumento de control.
Culpabilidad	Se desplaza la responsabilidad individual por la peligrosidad del sujeto. Se castiga al individuo por su condición o ideología, no por un acto probado.	Se elimina la exigencia de dolo o culpa, instaurando un Derecho Penal del autor contrario a la dignidad humana y a la igualdad ante la ley.
Proporcionalidad	Se justifican penas excesivas y desmedidas en nombre de la seguridad o la prevención.	Se rompe el equilibrio entre delito y sanción, legitimando un castigo desproporcionado e irracional, incompatible con la justicia constitucional.
Humanidad de las penas	El infractor es tratado como enemigo despojado de derechos; se aceptan medidas inhumanas, regímenes carcelarios degradantes y penas sin finalidad resocializadora.	Se vulnera la dignidad humana (art. 12 C.P.) y se transforma la pena en una herramienta de exclusión y venganza estatal.
Intervención mínima	Se abandona el principio de última ratio, expandiendo el Derecho Penal a cualquier conflicto o riesgo potencial.	El sistema penal se sobrecarga y pierde legitimidad, pues se usa el castigo como medio de control social general, contrario a la racionalidad del garantismo.

Fuente: Elaboración propia.

En definitiva, la TDPE constituye una profunda y grave amenaza para los límites del ius puniendi en un Estado Social de Derecho (ESD), pues su naturaleza está dada en ser mecanismo de exclusión más que en proteger bienes jurídicos.

De igual manera, el distinguir entre ciudadanos y enemigos, este modelo despoja a ciertas personas de sus derechos fundamentales y rompe los valores de igualdad, dignidad y debido proceso; pilares del ESD.

2.4.4. Conciliación teórico-práctica: El Terrorismo Digital en Colomba.

El Derecho Penal del Enemigo (DPE) constituye una teoría en la que confluyen notables críticas; sin embargo, su importancia radica precisamente en haber visibilizado prácticas punitivas

y arbitrarias que, aunque negadas desde el plano teórico, persisten dentro de los ordenamientos contemporáneos.

La TDPE, como se ha reiterado en diversas oportunidades, no es una finalidad del profesor Jakobs, no es su precursor; por el contrario, con esta teoría busca visibilizar una situación que -para el momento- el Derecho Penal estaba generando sin ningún tipo de réplica.

Por ello, menciona "hasta me resultaría agradable que pudiese disolverse la detestable imagen Derecho Penal del enemigo; ahora bien, no veo ninguna posibilidad de una disolución incondicionada, por ello intentó conocer y dar a conocer que es lo que pasa, aunque sea detestable" (Jakobs G, 2007b, p. 162)

Con esto en mente, la gravedad del fenómeno no nace de la teoría planteada sino de la existencia fáctica que de ella se deriva.

La TDPE se infiltra dentro del propio sistema penal, legitimando prácticas de exclusión bajo un aparente criterio de legalidad, operando de manera silenciosa en la práctica, pues se constituye como último recurso del Derecho Penal, cuando los demás medios son insuficientes, su objetivo: la función de aseguramiento del orden jurídico

No obstante, esto no quiere decir que Colombia adopte la TDPE de manera pura, por el contrario, al encontrase cimentado en un ESD reproduce parcialmente algunos de sus efectos, como consecuencia de las tensiones inherentes a la naturaleza del Derecho Penal que fluctúa entre la libertad vs la seguridad.

En efecto, el ESD al querer enfrentar aspectos del orden social o constitucional puede incurrir en respuestas punitivas segadas en elementos anticipatorios, incluso excluyentes propios de la TDPE.

Sin embargo, dicho resultado puede ser neutralizado por el sistema de contrapesos del poder público de la Constitución de 1991; así como, los principios que edifican al ESD, tales sistemas de contención como: control judicial, la supremacía constitucional, el principio pro homine, los derechos fundamentales, el bloque de constitucionalidad, etc.

Son mecanismos de corrección interna que impiden que el poder punitivo desborde en su práctica una TDPE pura.

Así, cuando esta teoría logra infiltrarse en el ordenamiento jurídico, el propio ESD opera como antídoto limitando su alcance a su mínima expresión o fragmentando sus postulados, sin que pueda aplicarse en su totalidad.

A la luz de lo expuesto, existen manifestaciones prácticas de la TDPE dentro de un sistema formalmente garantista, por consiguiente, instrumentos como la matriz permiten identificar los fundamentos teóricos sobre los que se edifica, posibilita evidenciar las tensiones preexistentes y aplicar mecanismos para su neutralización.

En verbigracia, la ausencia de tipificación del fenómeno del TDig encamino a que se evaluaran las políticas públicas del periodo 2020 a 2025 concernientes a CONPES 3995 de 2020 y 4144 de 2025 por ser el escenario más cercano frente al desarrollo de amenazas digitales en el que podría expresarse lógicas de control y prevención de la TDPE.

En primer, lugar, la aplicación de la matriz en cuanto al CONPES 3995 (Política Nacional de Seguridad Digital) se advierte que introduce mecanismos de vigilancia preventiva y distinciones entre actores confiables y amenazas, configurando un esquema de gestión del riesgo con una puntuación de 2.125 en la matriz.

Por su parte, el CONPES 4144 (Estrategia Nacional de Inteligencia Artificial) profundiza esta tendencia con un promedio menor de 1.875, trasladando la prevención del daño a un plano algorítmico de detección anticipada por parte de la institucionalidad.

Ambos documentos se encuentran en una tendencia hacia un funcionalismo sistemático lo que refleja que no existe, en primer lugar, lógicas punitivas por cuanto su órbita se cimienta en el derecho administrativo; es decir, no existe un enemigo en el estricto sentido de la TDPE, sino que se diluye en un riesgo administrable por el Estado, en pro de garantizar una seguridad digital para los distintos actores que interactúan en el Ciberespacio.

En este caso no se plantea una expulsión del ordenamiento jurídico ordinario del actor, sino una vigilancia constante del Estado con respecto al uso de las nuevas tecnologías para evitar futuros daños, en estas políticas de manera implícita se busca administrar y garantizar un comportamiento adecuado, por lo que el enemigo debe ser adoptado desde el riesgo, en otras palabras ya no es una-no persona- es un sujeto de gestión, vigilado, prevenido y administrado por el Estado.

La sanción queda como superada por la administración y la administración se presenta como cuidado. Como bien explica Shoshana Zuboff (2019), esta combinación Estado y tecnología hace que la prevención sea un nuevo modo de gobierno; la seguridad se autojustificá y vigila en nombre de la protección.

Michel Foucault (2007) desarrolló el argumento de que el poder actual ha dejado de necesitar la exclusión como medio para el dominio y es suficiente con la regulación de la vida. La biopolítica deviene ciberpolítica y el enemigo se transforma en el dato, en la anomalía dentro de un sistema informacional. El Estado no sólo deja de castigar la desviación, sino que sigue la variación.

Según Tuset (2024) “La vigilancia en la era digital se asemeja cada vez más al panóptico foucaultiano, donde la posibilidad de una observación constante influye en el comportamiento, incluso si la observación no es continua.”

De este modo, el Estado colombiano no adopta una TDPE, pero incorpora de manera reducida sus efectos simbólicos y funcionales en la gestión de la seguridad digital.

Ahora, no deviene de este trabajo de investigación propender o incluso determinar si la práctica punitiva de la TDPE resulta más eficaz y apropiada que el modelo garantista en el entorno digital. La cuestión central, radica en dar cumplimiento a los mandatos constitucionales, que la Constitución y la Corte Constitucional Colombiana ha previsto con fuerza vinculante dentro del sistema penal.

La racionalidad preventiva, de las políticas comparadas, debe dejar de estar anclada a la mera gestión técnica del riesgo, debe supeditarse en el marco del Estado Social de Derecho (ESD) requiere una mutación en el sentido de una seguridad digital garantista, en la que la protección de amenazas digitales no se logre en detrimento de los derechos fundamentales, sino más bien a la luz de ellos.

Lo que requiere entre otras cosas, asumir que la seguridad, en el plano digital, no es una mera finalidad técnica sino una categoría jurídica que necesita ser interpretada atendiendo los principios constitucionales de legalidad, proporcionalidad y dignidad humana, parámetros que ya han sido abordados por pronunciamientos internacionales como los tribunales europeos.

Una política pública efectiva y democrática, en procura de lo digital no puede fundarse en la opacidad de los algoritmos, ni en la lógica del control total, sino en la transparencia algorítmica, el control judicial efectivo y la responsabilidad institucional en la cuestión del tratamiento de los datos.

Por último, al comparar ambos documentos se observa que hay una tendencia en descenso sobre lógicas punitivas o de control y un avance progresivo en la inclusión de un enfoque garantista. El último CONPES se encuentra en un punto de madurez institucional ya que ha asumido el desarrollado de los derechos fundamentales de la ciudadanía como eje en el marco de la inteligencia artificial.

En este sentido, el gran reto consiste en saber traducir el reconocimiento formal de los derechos en otros mecanismos reales de control, supervisión y responsabilidad estatal de la esfera pública que de alguna manera contribuyan a construir una verdadera seguridad digital con rostro humano.

Esto de igual manera, debe darse en el ejercicio del ius puniendi, subordinado de manera categórica a los principios del ESD, entre ellos la dignidad humana, los cuales, no son simbólicos u opcionales, deben prevalecer de manera integral en la práctica penal sin excepción, pues son mandatos de obligatorio cumplimiento.

Diferente sería la situación ante un Estado de Derecho, donde el hombre está supeditado a la ley, la mera existencia de la legalidad bastaría para legitimar la acción penal. Pero en un ESD el Derecho Penal no se agota en el principio de legalidad, requiere observarse desde criterios supranacionales.

En efecto, este criterio supranacional, que da vida y estructura a todo el sistema jurídico colombiano, determina que las políticas criminales y las prácticas judiciales deben ajustarse bajo la protección de los derechos fundamentales, impidiendo que la excepción se normalice bajo el supuesto de la seguridad o de eficacia.

El reto del Estado colombiano, se encuentra frente a conductas particularmente graves que vulneran de manera latente el pacto social, pues debe buscar conciliar la seguridad pública con las garantías fundamentales, cuyo criterio orientador se encuentra en la dignidad, adoptando un Derecho Penal como mecanismo de control social, pero más como instrumento de garantías y no de venganza.

En este punto, como debería entonces el ESD enfrentar amenazas digitales que trascienden el riesgo administrativo y se encuadran como conductas punibles que repercuten en la vida social de las personas; en otras palabras, ¿Cómo responder penalmente a riesgos digitales que todavía no son delitos, sin caer en la lógica de la exclusión de la TDPE que pretendía superar?

Es claro que estas conductas punibles no van a desaparecer por cuanto comprenden una afectación directa al sistema social, no obstante, el Estado no puede reaccionar ante ellos de manera desmedida pues estaría al mismo tiempo desconociendo su base fundacional. Esta situación comienza a visibilizar los limites frente garantismo penal cuando esta frente a transformaciones del mundo contemporáneo.

En verbigracia, la política pública no basta para neutralizar la amenaza latente que es el TDig.

El ESD no puede permanecer inerte ante la apropiación simbólica y control estratégico de las circulación de información, la manipulación psicológica de las masas, la desestabilización

social generada por campañas de desinformación, e incluso la propaganda que actores pueden desplegar en el Ciberespacio, pues desestabilizan el orden social; pero tampoco puede responder desde la exclusión y el desarrollo de la categoría de -no persona-.

El garantismo cuyo principal exponente es Luigi Ferrajoli (1995) busca limitar el ius puniendi del Estado, así como proteger los derechos fundamentales frente a la arbitrariedad que ha de presentarse en el ejercicio del poder.

No obstante, la sociedad contemporánea se caracteriza por la complejidad, la globalización y la digitalización de los conflictos, lo que ha transformado radicalmente las condiciones de ejercicio del poder punitivo del Estado.

Se prevé, bajo este contexto la tensión entre la urgencia de cuidar la sociedad y la obligación de observar los márgenes constitucionales del poder punitivo, lo cual, constituye el origen de la crítica que Silva Sánchez (2001) frente al garantismo penal clásico.

Silva Sánchez (2001) parte de la crisis del Derecho Penal clásico o liberal, por cuanto su implementación desde la Revolución Francesa a la edad contemporánea ha tenido que dilatarse a las necesidades sociales que en la actualidad se deriva, pues no son los mismos bienes jurídicos de antaño lo que en la actualidad se protegen y esas garantías irrestrictas han cambiado, por ejemplo, el principio de legalidad.

Silva Sánchez comienza con la idea de que el garantismo clásico fue pensado para una sociedad consolidada con riesgos previsibles y delitos materiales, pero hoy con la globalización se está ante una sociedad del riesgo (Beck, 1998).

Una sociedad atravesada por riesgos difusos —tecnológicos, globales y digitalizados— que ya no pueden afrontarse adecuadamente, no puede resolverse desde las categorías dogmáticas clásicas.

Desde su mirada, el garantismo ferrajoliano es una doctrina de resistencia formal, preocupada únicamente por la limitación del castigo y sin la posibilidad de ofrecer soluciones jurídicas ante los nuevos daños sociales. Ahora, no quiere este autor edificar un rechazo al

garantismo; por el contrario, busca superar esta crítica para una mayor adaptación de la teoría a las nuevas realidades sociales que trae el progreso.

En este sentido, Silva Sánchez denuncia que la aplicación estricta del garantismo ha dado paso a una inmovilidad normativa que ha llevado al Derecho Penal a no intervenir, muy a pesar de la latente afectación de bienes jurídicos claves. Lo anterior, es dado por el principio de mínima intervención o el Derecho Penal como ultima ratio, donde no hay cabida para una expansión sino su acotamiento en el tiempo.

A pesar de ello, conforme la sociedad ha avanzado se ha constatado por parte del autor una tendencia clara de abrirse hacia nuevos tipos penales; así como una agravación de los ya existentes dentro del marco de garantías clásica.

De ahí que la "ampliación de los espacios de riesgos jurídico-penalmente relevantes, la flexibilización de las reglas de imputación y la relativización de los principios político-criminales de garantía no serían sino aspectos de esta tendencia general, a la que cabe referirse con el término «expansión»" (Silva Sánchez, 2001, p. 20).

Es así como, existe una antinomia frente a la intervención mínima y las crecientes necesidades que requiere la sociedad; porque la expansión del derecho penal dentro de la teoría del garantismo es presentada como un pecado para la estatalidad.

Sin embargo bajo parámetros racionales, el garantismo penal debe dejar esa dinámica de inacción (que impide al Estado responder ante nuevas formas de criminalidad que se desarrollan en una sociedad de riesgo) y comenzar a regularla los nuevos desafíos que se presentan bajo los marcos constitucionales que desarrolla.

El problema para Silva Sánchez (2001), no deriva en las garantías, sino en la falta de dinamismo de su aplicación por parte del Estado frente al panorama actual; dado que, el crimen implica estructuras difusas, colectivas y trasnacionales.

Ante esta realidad, el jurista sostiene que el Estado deberá contener una doble función:

Figura 35.

Función del Estado en el Garantismo Activo.

Fuente: Elaboración en Napkin con base en Silva Sánchez (2001)

Con ello, la expansión del Derecho Penal, puede ser un problema o contrariamente una solución a los nuevos intereses que demandan protección penal; a tal efecto, Silva Sánchez (2001) advierte que esto no puede observar criterios arbitrarios donde el Derecho Penal se convierta en la primera ratio, antes bien debe atender a razones "razonables" justificando su expansión.

Estas razones son: la emergencia de nuevos intereses sociales, los riesgos contemporáneos que derivan del progreso (sociedad de riesgo); por último, la inseguridad colectiva que acompaña a tales fenómenos (Cárdenas Bonilla, 2012).

A diferencia de ello, la expansión del derecho penal pierde legitimidad (razones irrazonables) cuando responde a la tendencia del populismo punitivo, es decir, cuando el castigo se convierte en una reacción primitiva o mediática para calmar la opinión pública.

En pocas palabras, cuando surge simplemente la búsqueda de culpables y el ciudadano no es más que un sospechoso permanente; o cuando se convierte en una utilización del castigo,

convirtiendo al Derecho Penal en un mecanismo de control político o social en lugar de en un medio de justicia (Cárdenas Bonilla, 2012)..

Al aplicar esta teoría de Sánchez Silva (2001) frente al TDig, se tiene que es una manifestación nítida de dicha sociedad del riesgo, tal y como la planteaba Ulrich Beck (1986), pues este riesgo no procede en causas naturales, sino de la propia acción humana y del desarrollo tecnológico.

El TDig, representa una mutación ontológica del riesgo; ya que, su objetivo no es el daño físico inmediato, sino el colapso del vínculo social del propio tejido colectivo desde la guerra psicológica y cultural.

A partir de la instrumentalización de las plataformas, donde la agresión no se mide en bajas materiales, sino en pérdida de confianza comunicativa afectando un nuevo bien jurídico: la seguridad digital derivada de la seguridad pública.

En tal contexto, aparece el TDig como una transformación, como una mutación del terrorismo clásico: su finalidad no es la de causar destrucción física sino colapsar los sistemas simbólicos sobre los que se sostiene la convivencia, tales como la confianza, la verdad y la legitimidad institucional. La guerra se traslada del terreno físico al comunicativo y el lenguaje se convierte en el arma más poderosa.

Existe, entonces una apropiación simbólica y control estratégico de las circulación de información, la manipulación psicológica de las masas, la desestabilización social generada por campañas de desinformación, e incluso la propaganda que actores que desestabilizan al Estado Colombiano.

Este marco resulta especialmente útil para analizar expresiones contemporáneas del terrorismo en el entorno digital, dentro de las cuales se ubica la TDPE como una modalidad específica del riesgo tecnológico actual.

Hecha esta salvedad, el TDig ha sido abordado desde la TDPE, precisamente, por la forma contemporánea de esa lógica de enemistad; ya que, el terrorista digital no considera la legitimidad

del Derecho, se mueve en la clandestinidad y emplea los propios instrumentos de la libertad (la comunicación, la tecnología, la información) para deshacer los cimientos del pacto social.

Con ello, el TDPE no es la solución para ingresar al ordenamiento penal la figura del TDig, pues existe un peligro evidente de trasladar de la teoría a la práctica; ya que al conformar figuras como la del "terrorista digital" desde la lógica del "Derecho Penal del Enemigo", el Estado puede correr el riesgo de incurrir en una respuesta punitiva anticipada, en función de la sospecha o de la potencial peligrosidad del sujeto antes que por sus actos.

El TDPE no es, la presentación de una propuesta normativa de Jakobs, sino una descripción crítica de un hecho real: los Estados contemporáneos, ante francas amenazas importantes, aplican un derecho dual, uno para los ciudadanos y otro para los "enemigos" peligrosos (Jakobs G, 2007a).

Así, el propio autor advierte que la TDPE no constituye una vía adecuada para enfrentar el fenómeno analizado, razón por la cual su tratamiento debe dejarse de lado; en tanto dicho deslizamiento lleva a la erosión de los derechos fundamentales, pues se argumenta la restricción de libertades en nombre de la seguridad, que acaba al final debilitando los derechos fundamentales y con ello el ESD amparado por la Constitución de 1991.

Desde este punto de vista, el peligro no es sólo el TDig, sino también la reacción del sistema de Derecho a la TDig, pues si el Estado asume una lógica de guerra con el "enemigo digital", renuncia al principio de igualdad ante la ley y convierte el Derecho Penal en una máquina de control preventivo.

En definitva, la defensa de la seguridad acaba por reproducir la misma lógica que se pretende erradicar: la negación del derecho como un espacio de racionalidad y de garantías.

En consecuencia, resulta necesario desplazar el enfoque hacia Sánchez Silva (2001), donde se encuentran las herramientas conceptuales más pertinentes para comprender y responder a este riesgo quien plantea un modelo de garantismo penal dinámico o activo, frente a la figura del TDig,

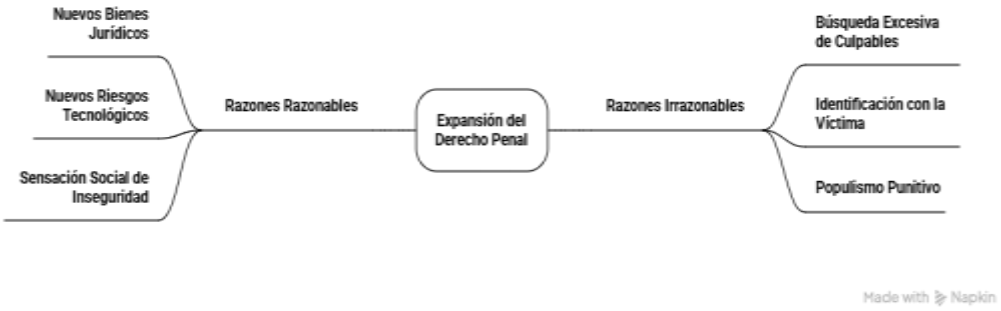
como inevitable expansión del Derecho Penal; pero sometido a parámetros razonables que justifique su introducción en el ordenamiento desde la proporcionalidad y legalidad.

Previamente, se identificará nuevamente que el TDig se configura como una amenaza directa al bien jurídico de la seguridad digital, concebida como una manifestación de la seguridad pública, en tanto busca salvaguardar a la población frente a actos dañinos para el pacto social, mediante el uso indebido de las TIC bajo el marco comunicacional digital (no físico, no técnico).

Como se advirtió, Silva Sánchez (2001) ha edificado parámetros: razonables e irrazonable para justificar si es factible la expansión del Derecho Penal ante una conducta que representa una afectación a los bienes jurídicos contemporáneos.

Figura 36.

Expansión del Derecho Penal para Jesús María Silva Sánchez

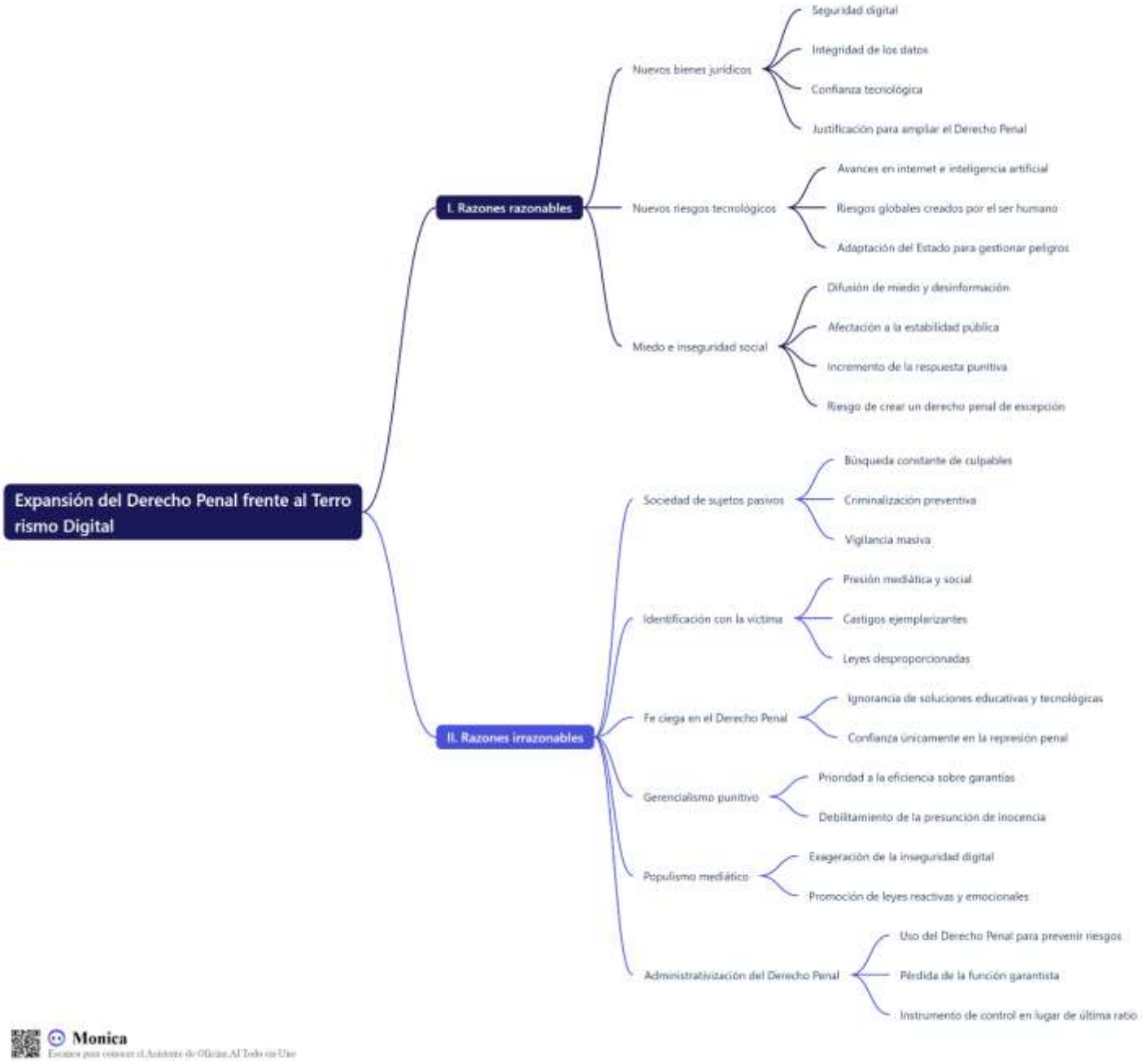


Fuente: Elaboración propia en Napkin con base en Silva Sánchez (2001).

Al aplicar dentro del Terrorismo Digital (TDig) como delito autónomo se tiene lo siguiente:

Figura 37.

Esquema de criterios razonables e irrazonables de la expansión del Derecho Penal frente al Terrorismo Digital



Fuente: Elaboración propia con asistencia de Mónica IA para la construcción del esquema.

Por consiguiente, el TDig simboliza un contexto ejemplar de la teoría de expansión del Derecho Penal, cuyos motivos para justificar su tipificación se encuentran dentro de los dos marcos.

Por un lado, su surgimiento se justifica por bases válidas que provienen de la necesidad de salvaguardar nuevos bienes jurídicos sean estos: la seguridad digital; así como, por la aparición de riesgos: el Ciberespacio como espacio sociotécnico que contempla diferentes riesgos por su naturaleza abierta, descentralizada y anónima, propio de los sistemas tecnológicos de la sociedad postindustrial y por la inseguridad colectiva que provoca.

Desde este punto de vista, la expansión del Derecho Penal se presenta como una respuesta útil y obligatoria, dirigida a proteger bienes fundamentales en un contexto globalizado y dependiente de la tecnología que debería desarrollar el ESD.

Ahora bien, también este mismo fenómeno pone en evidencia las razones irrazonables de expansión, dado que el tratamiento penal de la actividad terrorista delictiva a través de la tecnología viene incorporando: el populismo punitivo, el gerencialismo penal, la imputación desmesurada y la administración del Derecho Penal, propias o como consecuencia de la TDPE.

Cuando se esta ante razones irrazonables, es debido a que ya hay un delito inicial o porque se está fomentando una creación de tipos redundantes o simbólicos; esta sobrecriminalización no supone una protección adicional real, sino que responde a pulsiones coyunturales que son sobre todo mediáticas o emocionales, y que a su vez tienden a ver frustrada la arquitectura garantista del Derecho Penal.

En efecto, al multiplicar las figuras delictivas, se debilita el principio de legalidad (por vaguedad o amplitud de los tipos), se tensa la proporcionalidad (por el establecimiento de respuestas punitivas que son excesivas) se relativiza la culpabilidad (por extender la punición a ámbitos de mera sospecha o de peligrosidad), entre otras garantías clásicas que limitan de forma racional el ius puniendi.

Para el caso, el principio afectado es la legalidad, por dos razones: la primera de ellas es que bajo el principio del artículo 29 de la Constitución Política el legislador está obligado a describir de forma clara precisa y estricta el tipo penal.

El TDig contempla distintas estrategias para su materialización (véase Figura 13), es decir es un delito de naturaleza abierta, lo que hace imposible ofrecer un tipo penal típicamente cerrado en el sentido de cumplir con las exigencias de la taxatividad, del principio de seguridad jurídica y de previsibilidad de penas.

Por tanto, determinar un tipo penal autónomo de TDig llevaría a sancionar un tipo penal absurdamente extenso, que contravendría el principio de legalidad y daría un amplio margen para el intérprete, que no podría tener la certeza de determinar qué conductas concretas encajan o no con el tipo.

En segundo lugar, viene dado por el bien jurídico y la tipología preexistente, en el artículo 343 del Código Penal.

El TDig, al ser enfrentado al terrorismo tradicional solo introduce un nuevo medio comisivo; y una derivación de la seguridad pública, esto es la seguridad digital; por lo tanto su reconocimiento como delito autónomo deriva en el desarrollo de una conducta peligrosista propia del TDPE y comporta una conducta duplicada del tipo base en el ordenamiento penal.

Tabla 9.

Dogmática Penal del Terrorismo Tradicional vs el Terrorismo Digital.

Elemento dogmático	Terrorismo tradicional (Art. 343 C.P.)	Terrorismo digital (TDig)
Sujeto activo y pasivo	Sujeto activo indeterminado (cualquiera puede ser autor). Sujeto pasivo: la colectividad, la población en general o una parte de ella.	Sujeto activo igualmente indeterminado; puede operar individualmente o mediante redes globales anónimas. La víctima sigue siendo colectiva.
Tipo objetivo	Verbos rectores: *provocar o mantener* un estado de zozobra o terror en la población. El medio comisivo tradicional son explosivos, armas o actos violentos.	Los verbos rectores son idénticos: *provocar o mantener* zozobra o terror, pero el medio cambia: uso de TIC, redes sociales, IA, desinformación, manipulación algorítmica, ciberataques o sabotaje digital.
Resultado típico	Generación real o potencial de un estado de pánico o inseguridad colectiva.	Igual resultado: generar miedo o desestabilización social a través del entorno digital (viralidad, manipulación emocional, caos informativo).
Bien jurídico protegido	Seguridad pública: preservación del orden, confianza social y estabilidad institucional.	Seguridad digital como extensión de la seguridad pública; protege la confianza en los sistemas de información y comunicación.
Antijuridicidad	No requiere lesión efectiva, basta exposición al riesgo real de zozobra o terror.	Igual: basta el riesgo generado por el uso de tecnologías con potencial real de causar terror o desestabilización.
Tipo subjetivo	Delito doloso: el agente conoce y quiere producir terror mediante medios idóneos.	Idéntico dolo, aunque el agente puede obrar de forma coordinada mediante IA, redes o bots automatizados.
Exclusión de conductas	No aplica a hechos del conflicto armado interno (art. 144 C.P.).	Tampoco aplica; los actos digitales cometidos por grupos armados se rigen por el DIH y normas especiales.
Tipicidad objetiva y legalidad	Conducta típicamente delimitada: medios violentos con potencial de causar estragos.	Conductas digitales muy variables y técnicamente diversas (hackeos, campañas, IA, criptomonedas, metaverso, etc.).

Fuente: Elaboración propia con base en los elementos desarrollado por la Sentencia Corte Suprema de Justicia, Sentencia SP13290-2014 del 1 de octubre de 2014, M. P. María del Rosario González Muñoz)

La anterior comparación, permite concluir que para generar una expansión razonable del TDig, debe enmarcarse en el artículo 344 del Código Penal; toda vez que, al no cambiar la estructura base, sino el medio de ejecución no el fin, constituye una modalidad agravada al mantener la unidad del bien jurídico.

Frente al peligro concreto se aumenta su potencial de riesgo ante el entorno digital, justificando su aumento de pena, garantizando su coherencia sistemática y el principio de legalidad del ordenamiento, pues no modifica el injusto penal, amplía su alcance a las nuevas necesidades y riesgos de la sociedad contemporánea.

De este modo, el TDig es un indicador de la necesidad de una ampliación razonable: es un fenómeno lesivo y real, pero no nos ofrece un nuevo bien jurídico, sino una nueva forma de afectar

a ese mismo bien —la seguridad pública— que hoy debe, eso sí, referirse en su manifestación digital (la seguridad digital).

El análisis del TDig dentro del marco del Derecho Penal colombiano requiere comprender cómo las Tecnologías de la Información y la Comunicación (TIC) transforman los elementos clásicos del delito sin alterar su estructura dogmática esencial.

El uso de medios tecnológicos como instrumentos de agresión simbólica y psicológica redefine la escala del riesgo, la forma de imputación y la dimensión del bien jurídico protegido, generando una expansión funcional del Derecho Penal.

Sin embargo, esta expansión —como advierte Jesús-María Silva Sánchez (2001)— solo puede considerarse legítima cuando responde a causas "razonables", es decir, cuando preserva la racionalidad, la proporcionalidad y la legalidad como límites del ius puniendi.

Tabla 10.

Implicaciones de la comisión del terrorismo mediante las TIC

Dimensión analítica	Descripción del fenómeno en el entorno digital	Consecuencias jurídicas y dogmáticas
1. Medio comisivo digital	El terrorismo digital sustituye la violencia física por la violencia simbólica o informacional. Emplea redes sociales, algoritmos, IA, metaverso.	Transforma el tipo objetivo: el resultado (zozobra o terror colectivo) sigue siendo el mismo, pero el medio comisivo se amplía. Requiere reconocimiento como agravante dentro del art. 344 C.P., no un tipo autónomo. Refleja la *expansión razonable* del Derecho penal
2. Imputación subjetiva (dolo)	El anonimato, la automatización y la acción en red dificultan probar el conocimiento y la voluntad del autor. Puede existir dolo indirecto o eventual, orientado a provocar terror mediante manipulación masiva de información.	Se mantiene el dolo, pero la idoneidad tecnológica del acto debe probarse. La imputación requiere criterios objetivos (alcance, contexto, propósito).
3. Territorialidad y competencia penal	El ciberespacio disuelve los límites estatales: un acto puede ejecutarse en un país y generar efectos en otro. Predomina la transnacionalidad del riesgo.	Exige cooperación internacional y coordinación judicial. No obstante, la extensión extraterritorial del *ius puniendi* debe mantenerse bajo control constitucional para evitar una *expansión irrazonable*.
4. Riesgo de administrativización	El uso de TIC promueve el control preventivo estatal (vigilancia digital, monitoreo algorítmico, predicción de amenazas). Esto difumina las fronteras entre la prevención administrativa y la punición penal.	Peligro de caer en lógicas del Derecho penal del enemigo, castigando por peligrosidad y no por hechos. La agravante —no el tipo autónomo— permite delimitar objetivamente la respuesta penal sin desbordar la legalidad.
5. Bien jurídico y legitimidad punitiva	La seguridad pública se extiende al entorno digital: seguridad digital como confianza en los sistemas de información y estabilidad institucional.	No surge un nuevo bien jurídico, sino una extensión funcional del existente. La agravante fortalece su protección sin romper la unidad del sistema. Es expresión del garantismo penal dinámico

Fuente: Elaboración Propia.

En conclusión, el TDig debe ser comprendido como una forma específica de ejecución del terrorismo que se caracteriza por su condición dinámica inherente de los entornos tecnológicos, la cual, no se consuma en un acto único, sino en secuencias reiterables, escalables o acumulativas que amplifican el daño y aceleran la producción social del miedo.

Ese desarrollo progresivo aumenta el peligro concreto, redefine la escala de imputación y potencia la capacidad de desestabilización, pero no altera el núcleo estructural del injusto, porque la finalidad terrorista y el bien jurídico protegido permanecen idénticos.

Lo digital introduce un medio comisivo tecnológicamente cualificado, no un objeto jurídico distinto; de ahí que la respuesta penal adecuada no sea crear un nuevo delito, sino ajustar funcionalmente el alcance del tipo vigente para abarcar estos modos contemporáneos de realización.

Esta vía evita fórmulas indefinidas que comprometan taxatividad y previsibilidad, y se mantiene dentro de lo que Silva Sánchez denomina una expansión razonable del Derecho Penal: una ampliación limitada, racional y proporcional del sistema frente a riesgos reales de la modernidad, sin inflación simbólica de tipos ni ruptura de las garantías que legitiman el ius puniendi.

3. Formulación de hipótesis

Entre 2020 a 2025, el tratamiento jurídico-penal del Terrorismo Digital (TDig) en Colombia ha evidenciado una tendencia hacia la incorporación de rasgos de la Teoría del Derecho Penal del Enemigo (TDPE) de Günter Jakobs, observable en el fortalecimiento de las sanciones, la creación de nuevos tipos penales y la flexibilización de garantías procesales frente a conductas cibernéticas consideradas amenazas al Estado.

La extensión de la utilización de las Tecnologías de la Información y la Comunicación (TIC), especialmente después del advenimiento de la pandemia de COVID-19, ha propiciado formas alternativas de criminalidad mediante las que actores terroristas han entrado en el Ciberespacio con la intención de desestabilizar el mismo.

Esta nueva realidad ha llevado a que el Estado colombiano debe adaptar sus mecanismos de persecución penal a lo que son escenarios no físicos, sino digitalizados, lo que presenta retos desconocidos para el Derecho Penal clásico.

La hipótesis planteada es de tipo explicativa; ya que, establece una relación causal entre la incorporación de rasgos de la Teoría del Derecho Penal del Enemigo (TDPE) de Günter Jakobs y la evolución del tratamiento jurídico-penal del Terrorismo Digital (TDig) en Colombia entre 2020 a 2025.

4. Tratamiento de categorías

4.1. Terrorismo Digital (TDig).

La conceptualización de esta tipología, deriva de expresiones propias de la cibercriminalidad, apropiadas al cambio del terrorismo en el Ciberespacio (ciberterrorismo). Dentro de este fenómeno pueden distinguirse dos vertientes principales: El terrorismo informático y el Terrorismo Digital (TDig).

Por un lado, se encuentran los delitos cibernéticos dependientes (cyber-dependent crimes), que implican el uso directo de sistemas informáticos como medio esencial para la conducta, por ejemplo, el sabotaje cibernético o los ataques contra redes e infraestructuras críticas.

Por otro lado, están los delitos habilitados por la tecnología (cyber-enabled crimes), en los cuales las herramientas digitales —especialmente las redes— no constituyen el fin en sí mismo, pero sí potencian o facilitan conductas ya conocidas por el ordenamiento jurídico penal.

Es precisamente, en esta segunda dimensión donde se ubica el Terrorismo Digital (TDig), entendido como una modalidad que aprovecha el entorno tecnológico para amplificar fines y efectos terroristas, a partir de canales digitales como el internet "para difundir propaganda, recaudar fondos y blanquear dinero, reclutar y entrenar miembros, comunicarse y conspirar y lanzar ataques mientras los gobiernos intentan contrarrestarlos y atraparlos utilizando medios tradicionales" (Weimann, 2006, traducción propia p. 6)

4.2. Teoría Derecho Penal del Enemigo.

La Teoría del Derecho Penal del Enemigo, "es el conjunto de normas excepcionales que se dirige a individuos que se han apartado de forma duradera del derecho, es decir, que no reconocen la vinculación del sistema jurídico"(Almeyda, 2015, p. 111).

Con este derecho no se busca mantener la vigencia de la norma, pues no existe expectativa a mantener (el individuo ya no forma parte del sistema), se pretende neutralizar un peligro futuro de quien ha decidido no cumplir su rol; luego, no es un ordenamiento de comunicación normativa

sino un instrumento de aseguramiento que no reprocha las conductas punibles del pasado sino las futuras amenazas.

Es decir, una función meramente instrumental de seguridad para evitar que el enemigo cause un daño irreparable al pacto social; "lo que se busca es la neutralización del peligro futuro de quien ha decidido no vivir en sociedad" (Jakobs G, 2003, p. 49).

4.3. Estado Social de Derecho (ESD).

El Estado Social de Derecho (ESD), es un modelo de organización política cuyo eje se encuentra en la dignidad humana, el principio de igualdad material, la defensa de los derechos fundamentales y la limitación del poder punitivo del Estado.

La Constitución política define a Colombia en su artículo 1 como un Estado Social de Derecho (ESD)."Fue ésta una de las mayores innovaciones introducidas en 1991, pues ella constituye una norma fundamental o estructural del Estado, de aquellas que configuran la esencia misma del Estado colombiano "(Villar, 2007, p. 73).

Según la Corte Constitucional en Sentencia T-421 de 2017 establece que "El principal objetivo del Estado Social de Derecho (ESD) es garantizar la eficacia de los derechos. Por consiguiente, no se puede dar prevalencia a los procedimientos, ni al instrumento procesal, sobre el derecho sustancial" (Corte Constitucional, 2017b, M. P.: Iván Humberto Escrucería Mayolo.)

En este modelo, el Derecho Penal actúa como última ratio, actuando meramente cuando no se han resuelto por otros mecanismos de resolución, pero siempre dentro de unos límites desde aquellos marcados por el principio de legalidad, el debido proceso, la presunción de inocencia y la proporcionalidad de las penas.

5. Marco metodológico en la investigación

El presente trabajo de investigación, se edifica en una estructura de carácter jurídico-analítico, orientado a examinar desde la hermenéutica el fenómeno del TDig y su tratamiento en el ordenamiento colombiano a la luz de los postulados de la TDPE de Günter Jakobs y sus tensiones con los principios del Estado Social de Derecho (ESD).

La ruta metodológica propuesta busca garantizar un análisis riguroso, coherente y sistemático adaptada a la nueva realidad social que ofrece el Ciberespacio, para ello, como fundamento teórico se tiene presente la obra denominada "*Metodología de la investigación social y jurídica"* de las autoras Myriam Sepúlveda López y Nancy Solano de Jinete (2008).

Con el fin, de desarrollar en este acápite un modelo de análisis jurídico-interpretativo, que integra los enfoques dogmático, normativo y político-criminal, propios de la investigación jurídica aplicada.

De igual manera, la obra de Hernández Sampieri, Fernández y Baptista (2014), "*Metodología de la investigación"*, se presenta como referente metodológico complementario. Su inclusión es decisiva ya que el modelo de Sampieri permite tener un referente sistemático y actualizado para formular elementos de enfoque, tipo, alcance.

La combinación de cada uno de los referentes metodológicos articula un camino coherente entre la dimensión jurídica y la dimensión científica de la investigación, garantizando un proceso analítico, riguroso y verificable.

5.1. Línea de Investigación

Según el Acuerdo 069 de 2022 de la Universidad Colegio Mayor de Cundinamarca, mediante el cual se actualizan las líneas institucionales de investigación, el presente trabajo de estudio se enmarca en la línea de investigación No. 2 denominada *"Estado, sociedad y cultura"* la cual comprende:

> Línea 02. Estado, sociedad y cultura: Aborda las problemáticas que surgen en los ámbitos social y público en aras por responder a las tensiones que se generan al momento de implementar los derechos a nivel nacional e internacional, la interseccionalidad, los estudios indígenas, estudios afro, estudios de familia, conflicto y sociedad, el valor del trabajo, la seguridad, la salud alimentaria e interculturalidad; el análisis de los estudios poblacionales, la circulación de saberes y construcción de identidades, el estudio de la ciudadanía y cultura política (Consejo Académico de la Universidad Colegio Mayor de Cundinamarca, 2022, p. 3)

Esta línea, al situarse en el campo de las relaciones entre el Estado, el derecho y la sociedad contemporánea, se articula al trabajo de investigación, en tanto el Terrorismo Digital (TDig) constituye una problemática emergente que desafía los fundamentos democráticos y los principios garantistas del Estado Social de Derecho (ESD).

El análisis del tratamiento jurídico-penal frente a esta amenaza no solo implica una reflexión sobre la eficacia de la norma penal, sino también sobre su impacto social, cultural y político, al cuestionar los límites entre la seguridad y las libertades públicas.

5.2. Método de Investigación

El presente trabajo adopta el método de investigación de carácter deductivo como eje orientador del análisis jurídico, en la medida en que parte de principios generales y teorías consolidadas (Terrorismo y TDPE) para llegar a conclusiones específicas sobre el tratamiento del TDig en el ordenamiento jurídico colombiano.

Según Rodríguez Jiménez y Pérez Jacinto (2017) exponen:

> Mediante la deducción se pasa de un conocimiento general a otro de menor nivel de generalidad. Las generalizaciones son puntos de partida para realizar inferencias mentales y arribar a nuevas conclusiones lógicas para casos particulares. Consiste en inferir soluciones o características concretas a partir de generalizaciones, principios, leyes o

> definiciones universales. Se trata de encontrar principios desconocidos, a partir de los conocidos o descubrir consecuencias desconocidas, de principios conocidos…(p.11)

Por consiguiente, el método deductivo hace que esta investigación transite de marcos teóricos generales y extensamente desarrollados hacia una propuesta concreta, como lo es, el Terrorismo Digital (TDig) en Colombia, en el periodo entre 2020 a 2025; garantizando así un análisis alongado y lógico de la problemática.

5.3. Forma de Investigación

El presente trabajo de investigación se desarrolla en una perspectiva teórico–práctica, puesto que combina la reflexión conceptual con la aplicación empírica en el análisis jurídico, tal como lo señala el investigador Gordillo Álvarez-Valdés (1985) “la teoría aclara la praxis y actúa sobre ella a partir de los saberes adquiridos a partir de ella misma” (p. 72).

En esta medida, la investigación no se reduce a una mera exposición doctrinal, sino que busca aplicar los referidos postulados de la Teoría del Derecho Penal del Enemigo (TDPE) de Günther Jakobs a partir de la matriz sugerida, para abordar la política pública colombiana, lo cual permite mostrar cómo empiezan a tomar forma en la práctica jurídica nacional.

Así mismo, tal y como enuncia Solano y Sepúlveda (2008), este tipo de investigación “es más formal y persigue la generalización en vistas a la elaboración de una teoría fundamentada en principios y leyes” (p. 141).

En este sentido, el trabajo no sólo busca realizar una aplicación normativa de la figura del Derecho Penal de enemigo, sino que reconoce ciertas pautas, o estructuras conceptuales que ayudan en la construcción de marcos interpretativos útiles en el fortalecimiento del pensamiento penal colombiano.

Lo anterior, se realiza mediante la interpretación y comprensión de la hermenéutica, por lo que su proceso de descubrimiento es de índole interpretativa a través de un análisis en estricto derecho.

Bajo este referente, no contempla el uso técnicas tales como entrevistas, encuestas (tipo sondeo de opinión) sino la técnica de recolección de información, a través de la revisión documental, como: otras investigaciones, normatividad, jurisprudencia y doctrina inherente al problema objeto de estudio.

5.4. Enfoque de Investigación

En coherencia con las doctrinantes Solano y Sepúlveda (2008), el paradigma cualitativo "insiste en la relevancia del fenómeno frente al rigor e intenta comprender la realidad dentro de un contexto dado" (p. 32).

De igual manera, Aranzamendi (2015) señala que la investigación cualitativa *"*está orientada hacia la descripción y la comprensión de una situación o fenómeno (caso del Derecho) a diferencia de la cuantitativa que se centra en la cuantificación, predicción y control*"* (p. 76),

En efecto, la presente investigación adopta un enfoque cualitativo, puesto que se intenta comprender e interpretar a fondo el fenómeno del Terrorismo Digital (TDig) y el tratamiento de este delito en el contexto del ordenamiento jurídico colombiano, de acuerdo a los postulados de la Teoría del Derecho Penal del Enemigo (TDPE) de Günther Jakobs y las tensiones que se producen con los principios del Estado Social de Derecho (ESD).

Conforme a ello, los autores Hernández, Collado, Lucio, Valencia y Torres (2014) señalan que las investigaciones teórico-cualitativas no se trabajan variables, sino categorías que permiten comprender el fenómeno estudiado, pues "hay un análisis común en todo estudio cualitativo: generar categorías o temas" (p. 422).

En esa línea, esta investigación organiza su análisis a partir de tres categorías centrales: la Teoría del Derecho Penal del Enemigo (TDPE), el Terrorismo Digital (TDig) y el Estado Social de Derecho (ESD).

5.5. Alcance de Investigación

El alcance de la presente investigación, desde la perspectiva de Roberto Hernández Sampieri, obedece a ser hibrida: es explicativa y correlacional, dado que busca esclarecer el fenómeno del Terrorismo Digital (TDig) en Colombia entre 2020 a 2025 relacionándolo con la aplicación de la Teoría del Derecho Penal del Enemigo (TDPE).

Frente al alcance explicativo Hernández, Collado, Lucio, Valencia & Torres (2014) disponen que:

> Los estudios explicativos van más allá de la descripción de conceptos o fenómenos o del establecimiento de relaciones entre conceptos; es decir, están dirigidos a responder por las causas de los eventos y fenómenos físicos o sociales. Como su nombre lo indica, su interés se centra en explicar por qué ocurre un fenómeno y en qué condiciones se manifiesta o por qué se relacionan dos o más variables (p.95)

Bajo este referente, la investigación ostenta un alcance explicativo porque busca analizar relaciones tanto conceptuales como causales entre el fenómeno del Terrorismo Digital (TDig) y la aplicación de los fundamentos teóricos de la Teoría del Derecho Penal del Enemigo (TDPE) en el contexto colombiano.

Por ello, al tener dos variables que se asocian entre sí es necesario también un alcance de tipo correlacional, Hernández, Collado, Lucio, Valencia & Torres (2014) frente a este enfoque manifiestan:

> Este tipo de estudios tiene como finalidad conocer la relación o grado de asociación que existe entre dos o más conceptos, categorías o variables en una muestra o contexto en particular. En ocasiones sólo se analiza la relación entre dos variables, pero con frecuencia se ubican en el estudio vínculos entre tres, cuatro o más variables. Para evaluar el grado de asociación entre dos o más variables, en los estudios correlacionales primero se mide cada una de éstas y después se cuantifican, analizan y establecen las vinculaciones(p.93)

Por consiguiente, el objetivo es establecer una relación entre estas variables y entender cómo se influyen mutuamente en el contexto específico, si existe o no posibles conexiones entre el auge del Terrorismo Digital (TDig) y el fortalecimiento de un enfoque penal con base en la identificación de sujetos considerados como enemigos del Estado.

5.6. Técnicas de Recolección de Investigación

En el presente trabajo investigación, se emplea un método de análisis documental., lo cual implica, un enfoque exhaustivo sobre la evolución del Terrorismo Digital (TDig) en Colombia y la posible relación con los principios de la TDPE, según las autoras Myriam Sepúlveda López y Nancy Solano de Jinete (2008) "se realiza a través de la consulta de documentos (libros, revistas, periódicos, memorias, anuarios, registros, constituciones, etc."(p.142)

La recopilación de datos selección e interpretación crítica de fuentes jurídicas, doctrinales, normativas y jurisprudenciales relacionadas con el Terrorismo Digital (TDig) y su tratamiento en el ordenamiento jurídico colombiano.

Este tipo de análisis permite examinar el fenómeno desde una perspectiva teórica y hermenéutica, sin recurrir a la recolección de datos cuantitativos, lo que posibilita la construcción de conocimiento interpretativo a partir de documentos legales y académicos.

En definitiva, este discurso metodológico se basa en una técnica jurídico-analítica y de tipo cualitativo- la cual prevé la comprensión y la interpretación del tratamiento del Terrorismo Digital (TDig) en Colombia a partir de los postulados de la Teoría del Derecho Penal del Enemigo (TDPE) de Günther Jakobs.

6. Conclusiones.

Durante el periodo comprendido entre 2020 a 2025, el tratamiento jurídico-penal del Terrorismo Digital (TDig) en Colombia no incorporó rasgos del Derecho Penal del Enemigo de Günter Jakobs.

La investigación reveló, a partir de la matriz aplicada, que el análisis de las políticas públicas —en particular los documentos CONPES 3995 de 2020 y CONPES 4144 de 2025— evidencia una orientación estatal hacia una lógica administrativa y preventiva; esta se expresa, en la gestión del riesgo, la cooperación institucional, la vigilancia anticipada mediante TIC y el control administrativo, más que en una expansión del poder punitivo.

6.1. La noción de enemigo se disuelve en la figura del riesgo en tanto que el TDig queda subsumido en un fenómeno administrable más que punible; dado su atipicidad; de allí que, el Estado Colombiano no castiga al enemigo sino que lo previene, lo controla y lo regula, por ello, la respuesta no retiene una lógica anticipatoria punitiva propia del TDPE en ese nuevo modelo de gobernabilidad digital.

6.2. En lo que respecta a la flexibilidad en el endurecimiento de las sanciones, la revisión determino que no existen referencias en la política criminal o legislativas que acojan, durante el periodo en cuestión, un agravamiento del tratamiento penal de las conductas subsumibles en conductas tipificadas como “TDig”.

Así como, un aumento de las penas por el mero hecho de hacer un uso de medios tecnológicos; es decir, sigue existiendo en el ordenamiento el tratamiento tradicional del terrorismo sin ningún cambio.

6.3. El TDig, presenta en la actualidad un alto grado de atipicidad penal, pues sus manifestaciones no se encuentran recogidas de manera integral dentro del marco jurídico vigente.

Esta ausencia de un tipo penal específico evidencia las limitaciones del Derecho Penal clásico para abordar fenómenos que trascienden la materialidad del delito y se desarrollan en entornos virtuales, descentralizados y globalizados.

6.4. Sobre esa base el estudio del tipo penal del artículo 343 del Código Penal el cual tutela la seguridad pública, le es admisible su adecuación tecnológica a partir de la identificación del medio comisivo.

Los elementos constitutivos del terrorismo tradicional siguen reproduciéndose integralmente en el entorno digital, lo único que se transforma es su canal, un nuevo escenario de confrontación simbólica y operativa, pero con el mismo propósito de infundir terror y alterar los cimientos del pacto social.

6.5. De la teoría conciliadora del garantismo activo de Jesús-María Silva Sánchez (2001) se obtiene precisamente la conclusión central: si el ordenamiento exige ajustar la respuesta a los riesgos del TDig, la defensa legítima es una expansión razonable del ius puniendi, o lo que es lo mismo, incorporar una agravante por uso de medios digitales dentro del terrorismo, pero no elaborar un tipo autónomo.

6.6. En lo que respecta a la flexibilización de garantías procesales, el periodo no refleja el establecimiento de regímenes de excepción específicos para conductas digitales que impliquen: inversión de cargas probatorias, abaratamiento de estándares de sospecha razonable, ampliación anómala de medidas intrusivas sin control judicial o debilitamiento de la presunción de inocencia.

Las medidas mencionadas en la política pública transitan fuera de las fronteras del proceso penal y conforme al Estado Social de Derecho.

6.7. Bajo la tipología de la cibercriminalidad, el ciberterrorismo posee dos vertientes: El terrorismo informático y el TDig; el primero, comprende el uso directo de tecnologías digitales, derivado de los ataques cibernéticos o de la guerra cibernética.

6.8. El segundo, engloba aquellos delitos tradicionales que se ven potenciados gracias a las nueva herramientas tecnológicas, no busca un daño técnico, busca utilizar canales digitales como instrumento fidedigno de coerción, intimidación o desestabilización.

6.9. El TDig, no necesita necesariamente de armas convencionales o de la ocupación física de un lugar, sino la apropiación simbólica y control estratégico de las circulación de información, la manipulación psicológica de las masas, la desestabilización social

generada por campañas de desinformación, e incluso la propaganda radical son suficientes para ocasionar caos, inseguridad o presión política.

6.10. El TDig no reconoce el orden jurídico, no se somete a las reglas del discurso democrático y opera desde la negación de la expectativa normativa, no se está ante un infractor común, sino un actor que utiliza la libertad comunicativa y tecnológica —los propios medios contemporáneos— para destruir sus cimientos, su manifestación natural: representa la antítesis del ciudadano normativo y encarna la ruptura entre el Derecho y la conducta socialmente esperada.

6.11. En este orden de ideas, el TDig es una representación del TDPE; pues su práctica encarna la lógica de la que nos habla Jakobs, que es aquella por la que el sujeto se autoexcluye del pacto normativo, renuncia a ser un ciudadano y se convierte en un riesgo permanente.

6.12. Sin embargo, el TDPE no es la solución para ingresar al ordenamiento penal la figura del TDig, pues existe un peligro evidente de trasladar de la teoría a la práctica; ya que al conformar figuras como la del "terrorista digital" desde la lógica del "Derecho Penal del Enemigo", el Estado puede correr el riesgo de incurrir en una respuesta punitiva anticipada, erosionando derechos fundamentales y con ello debilitan el ESD amparado por la Constitución de 1991.

6.13. Desde este punto de vista, el peligro no reside únicamente en el TDig como fenómeno criminal, sino también —y de forma especialmente sensible— en la manera como el Estado decide enfrentarlo.

El riesgo aparece cuando la reacción institucional se organiza desde una lógica de "enemigo digital", es decir, como si se tratara de una guerra; a partir de este escenario, el sistema jurídico tiende a relativizar derechos y desplaza el Derecho Penal hacia funciones de control preventivo.

Así, en nombre de la seguridad, puede terminar reproduciéndose aquello que se pretende combatir: la negación del Derecho como espacio de racionalidad, límites y garantías.

6.14. Frente a esta deriva deshumanizante del poder punitivo, cobra sentido la propuesta de Silva Sánchez, quien plantea un garantismo penal dinámico o activo; en su planteamiento, el Derecho Penal puede expandirse frente a nuevas realidades, pero debe hacerlo de manera racional, proporcional y compatible con la legalidad, sin crear tipos simbólicos ni inflacionarios que desdibujen la frontera de lo punible.

6.15. Este modelo reconoce que fenómenos como el TDig hacen inevitable cierta expansión del Derecho Penal, pero exige que dicha ampliación se someta a parámetros razonables de justificación, estricta proporcionalidad y respeto por la legalidad, de modo que la adaptación del sistema no implique la renuncia a sus fundamentos garantistas.

7. Alternativas de intervención y solución

Las estrategias que se desarrollan a continuación, se realizan en aras de conciliar la figura del Terrorismo Digital (TDig) frente a los principios constitucionales del Estado Social de Derecho (ESD); el comentado enfoque se aborda dentro de dos frentes complementarios estos son: Alternativas de intervención pedagógicas y sociojurídicas y alternativas de solución sociojurídicas, en aras de convertir los resultados aquí expresados en acciones prácticas de transformación de la cultura jurídica actual:

7.1. Alternativas de intervención sociojurídicas y pedagógicas

7.1.1. Programa Radial de la Universidad Colegio Mayor de Cundinamarca.

Figura 38.

Programa radial UCMC.

Fuente: Tomada del Programa Radial “Señal Mayor” (2025)

El programa radial fue grabado el 14 de agosto de 2025 y publicado el 2 de septiembre de 2025 por la Universidad Colegio Mayor de Cundinamarca con la moderación de la Doctora Myriam Sepúlveda López, directora de la Maestría en Derecho Penal.

A partir de la radio virtual de la Universidad Colegio Mayor de Cundinamarca se difundieron de manera accesible los principales conceptos y hallazgos teóricos generando una democratización en el conocimiento jurídico de categorías como el TDig, el Derecho Penal del Enemigo y el Estado Social de Derecho (ESD).

Este marco comunicativo logró reforzar, ampliar y sostener la comprensión de las categorías analizadas por estudiantes, egresados y docentes, propiciando así la reflexión crítica sobre la cultura digital desde la perspectiva penal y constitucional. En este contexto se logró visibilizar las nuevas formas de vigilancia, control y exposición que brotan de los entornos virtuales, así como los riesgos vinculados a la interacción y el manejo de las amenazas en el Ciberespacio, como lo es el TDig en un país como el colombiano.

Véase Anexo 2.

7.1.2. Clases Socialización: Derecho Penal del Enemigo y el Fenómeno del Terrorismo Digital.

Las clases serán impartidas en la Universidad Colegio Mayor de Cundinamarca y dirigidas a estudiantes, con la finalidad de desarrollar sesiones que transmitan los contenidos teóricos del trabajo investigativo.

Las clases propugnan por un pensamiento analítico y crítico a los futuros profesionales de derecho, capacitando a los futuros profesionales en desafíos emergentes del Derecho Penal en el Ciberespacio como en el conflicto garantista-punitivo contemporáneo materializado por el Derecho Penal del Enemigo (DPE), proporcionando herramientas para su comprensión integral.

El valor de ello radica en el hecho de formar una conciencia jurídica que estructure la prevención del riesgo y la defensa de los derechos fundamentales, contribuyendo así a una concepción penalista de la seguridad en la era digital.

Véase Anexo 4.

7.1.3. Artículo resultado de la investigación denominado: "El Terrorismo Digital en Colombia: entre el Derecho Penal del Enemigo y el Estado Social de Derecho".

Desde la óptica académica, se propone como alternativa de solución un artículo resultado de la investigación denominado "*El Terrorismo Digital en Colombia: entre el Derecho Penal del Enemigo y el Estado Social de Derecho*", presentado a la Misión Jurídica, Revista de Derecho y Ciencias Sociales perteneciente a la Universidad Colegio Mayor de Cundinamarca, con el objetivo de difundir el análisis desarrollado en esta investigación dentro de comunidad academia, contribuyendo de esta manera al debate doctrinal en relación a la aplicación de la Teoría del Derecho Penal del Enemigo (TDPE) en el contexto de la era digital.

Su contribución se encuentra en la reflexión jurídica, contribuye a incrementar el diálogo entre academia y Estado, aportando criterios de interpretación constitucional que puedan servir para las futuras reformas legislativas, políticas o judiciales.

Véase Anexo 3.

7.1.4. Guía del Derecho Penal del Enemigo + Matriz analítica.

La guía metodológica del Derecho Penal del Enemigo, acompañada de la matriz analítica desarrollada en la investigación, constituye una herramienta de evaluación jurídica aplicada que materializa los aportes teóricos del estudio en un instrumento operativo de análisis y verificación.

Su funcionamiento reside en la posibilidad de identificar, medir y contrastar hasta qué punto las políticas públicas, las leyes o las propias actuaciones estatales en materia de seguridad digital integran aspectos propios de la TDPE.

La Guía será entregada al Consultorio de la Universidad Colegio Mayor de Cundinamarca, a fin de proporcionar al consultorio una metodología verificable y replicable que posibilita la práctica del control democrático y la asesoría jurídica crítica de las normas, proyectos de ley o políticas públicas frente a la TDPE, su sistematización permite ser una herramienta técnica y original de auditoría jurídica.

Véase Anexo 1 y 5.

7.1.5. Ponencia sobre el objeto de investigación.

Se pretende desarrollar ponencias en eventos o seminarios de la Universidad Colegio Mayor de Cundinamarca en aras de circular de manera pública los hallazgos de la investigación mostrando a la comunidad académica su relevancia, novedad y aporte.

Las preguntas, observaciones y sugerencias que se reciban puede ser una buena forma de afinar el análisis, extender la discusión teórica o mejorar la interpretación de los resultados, logrando, en definitiva, que la presente disertación gane firmeza.

Asimismo, su implementación abriría caminos para la investigación en aras de generar otro tipo de publicaciones o bien de redes de investigación académica; creando mayor experiencia en formas de comunicación jurídica y posicionamiento en el ámbito.

Véase Anexo 6.

7.2. Alternativas de solución sociojurídicas

7.2.1. Proyecto de ley sobre Terrorismo Digital (TDig).

Una primera alternativa de solución se orienta al fortalecimiento normativo del ordenamiento penal colombiano mediante la incorporación de una agravante específica para los casos en que el delito de terrorismo se cometa a través de medios digitales.

Su valía práctica reside en permitir a fiscales y jueces adecuar jurídicamente conductas reales que hoy se presentan en el ámbito digital, evitando omisiones de imputación y conduciendo a reafirmar la respuesta institucional frente amenazas digitales. Esta alternativa supone así una actualización técnica del Derecho Penal acorde con la era digital garantizando que la seguridad nacional teniendo presente los parámetros del Estado Social de Derecho (ESD), es decir, sin desbordar los márgenes constitucionales del poder punitivo.

7.2.2. Observatorio Nacional de Seguridad Digital y Derechos Digitales.

El fortalecimiento institucional exige la creación de un Observatorio Nacional de Seguridad Digital y Derechos Digitales integrado por entidades públicas, universidades, y organizaciones sociales. Este ámbito facilita articular la gestión del riesgo con la deliberación pública; siguiendo la teoría de la acción comunicativa de Habermas (1992), la legitimidad del poder estatal vendría dada por el consenso racional conseguido en la conversación social.

7.2.3. Plan de Estudios sobre Derecho Penal tecnológico.

Del mismo modo, es necesaria la incorporación en los planes de estudios de educación superior de contenidos sobre el Derecho Penal tecnológico, la ética digital y los derechos humanos en el Ciberespacio. Para Silva Sánchez (2001), la expansión del Derecho Penal contemporáneo hace necesario repensar y establecer los límites desde la enseñanza, introduciendo una enseñanza que sea crítica y que permita comprender las consecuencias de la sobre criminalización y del punitivismo digital.

Referencias

Constitución y leyes

Congreso de la República. (2000). *Código Penal, Ley 599 de 2000.* Disponible en http://www.secretariasenado.gov.co/senado/basedoc/ley_0599_2000.html

Congreso de la República. (2009). *Ley 1273 de 2009.* Disponible en https://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf

Congreso de la República de Colombia. (2018). *Ley 1928 de 2018 "Por medio de la cual se aprueba el Convenio de Budapest sobre la Ciberdelincuencia".* Diario Oficial No. 50.678 del 18 de julio de 2018. http://www.secretariasenado.gov.co/senado/basedoc/ley_1928_2018.html

República de Colombia. (1991). *Constitución Política de Colombia.* Asamblea Nacional Constituyente. https://www.constitucioncolombia.com/

Políticas públicas (CONPES) y lineamientos nacionales.

Consejo Nacional de Política Económica y Social (CONPES). (2011). *Lineamientos de política para ciberseguridad y ciberdefensa (Documento CONPES 3701).* Departamento Nacional de Planeación. https://colaboracion.dnp.gov.co/CDT/Conpes/Económicos/3701.pdf

Consejo Nacional de Política Económica y Social (CONPES). (2016). *Política nacional de seguridad digital (Documento CONPES 3854).* Departamento Nacional de Planeación. https://colaboracion.dnp.gov.co/CDT/Conpes/Económicos/3854.pdf

Consejo Nacional de Política Económica y Social (CONPES). (2020). *Política Nacional de Confianza y Seguridad Digital (Documento CONPES 3995).* Departamento Nacional de Planeación. https://colaboracion.dnp.gov.co/CDT/Conpes/Económicos/3995.pdf

Consejo Nacional de Política Económica y Social (CONPES). (2025). *Política Nacional de Seguridad Digital y Ciberdefensa 2025–2030 (Documento CONPES 4144).* Departamento Nacional de Planeación. https://colaboracion.dnp.gov.co/CDT/Conpes/Económicos/4144.pdf

Departamento Administrativo Nacional de Estadística (DANE). (2023). *Boletín técnico: Indicadores básicos de tenencia y uso de Tecnologías de la Información y las Comunicaciones – TIC en hogares y personas de 5 y más años de edad, 2023.* Bogotá, D. C. Recuperado de https://www.dane.gov.co/files/operaciones/TICH/bol-TICH-2023.pdf

Departamento Nacional de Planeación. (2023). *Estrategia Nacional Digital 2023–2026.* Recuperado de https://colaboracion.dnp.gov.co/CDT/Desarrollo%20Digital/EVENTOS/END_Colombia_2023_2026.pdf

Jurisprudencia Nacional Corte Constitucional y Corte Suprema de Justicia.

Corte Constitucional. (1992a). *Sentencia T-401 del 3 de junio de 1992.* Sala Plena. M. P.: Eduardo Cifuentes Muñoz.

Corte Constitucional. (1992b). *Sentencia T-406 del 5 de junio de 1992.* Sala Segunda de Revisión. M. P.: Ciro Angarita Barón.

Corte Constitucional. (1992c). *Sentencia T-414 del 29 de junio de 1992.* Sala Segunda de Revisión. M. P.: Ciro Angarita Barón.

Corte Constitucional. (1993). *Sentencia C-127 del 22 de abril de 1993.* Sala Plena. M. P.: Alejandro Martínez Caballero.

Corte Constitucional. (1995a). *Sentencia C-009 del 17 de enero de 1995.* Sala Plena. M. P.: Vladimiro Naranjo Mesa.

Corte Constitucional. (1995b). *Sentencia C-038 del 9 de febrero de 1995.* Sala Plena. M. P.: Alejandro Martínez Caballero.

Corte Constitucional. (1995c). *Sentencia SU-082 del 1 de marzo de 1995.* Sala Plena. M. P.: Jorge Arango Mejía.

Corte Constitucional. (1995d). *Sentencia C-566 del 30 de noviembre de 1995.* Sala Plena. M. P.: Eduardo Cifuentes Muñoz.

Corte Constitucional. (2001a). *Sentencia C-710 del 5 de julio de 2001.* Sala Plena. M. P.: Jaime Córdoba Triviño.

Corte Constitucional. (2001b). *Sentencia C-1064 del 10 de octubre de 2001.* Sala Plena. M. P.: Manuel José Cepeda Espinosa y Jaime Córdoba Triviño.

Corte Constitucional. (2002a). *Sentencia T-729 del 5 de septiembre de 2002.* Sala Séptima de Revisión. M. P.: Eduardo Montealegre Lynett.

Corte Constitucional. (2002b). *Sentencia C-916 del 29 de octubre de 2002.* Sala Plena. M. P.: Manuel José Cepeda Espinosa.

Corte Constitucional. (2004). *Sentencia T-1096 del 4 de noviembre de 2004.* Sala Plena. M. P.: Manuel José Cepeda Espinosa.

Corte Constitucional. (2010a). *Sentencia C-073 del 10 de febrero de 2010.* Sala Plena. M. P.: Humberto Antonio Sierra Porto.

Corte Constitucional. (2010b). *Sentencia C-936 del 23 de noviembre de 2010.* Sala Plena. M. P.: Luis Ernesto Vargas Silva.

Corte Constitucional. (2012). *Sentencia C-365 del 16 de mayo de 2012.* Sala Plena. M. P.: Jorge Ignacio Pretelt Chaljub.

Corte Constitucional. (2014). *Sentencia C-767 del 16 de octubre de 2014.* Sala Plena. M. P.: Jorge Ignacio Pretelt Chaljub.

Corte Constitucional. (2017a). *Sentencia C-108 del 22 de febrero de 2017.* Sala Plena. M. P.: Luis Ernesto Vargas Silva.

Corte Constitucional. (2017b). *Sentencia T-421 del 4 de julio de 2017.* Sala Plena. M. P.: Iván Humberto Escrucería Mayolo.

Corte Constitucional. (2019a). *Sentencia C-224 del 22 de mayo de 2019.* Sala Plena. M. P.: Cristina Pardo Schlesinger.

Corte Constitucional. (2019b). *Sentencia C-233 del 29 de mayo de 2019.* Sala Plena. M. P.: Luis Guillermo Guerrero Pérez.

Corte Suprema de Justicia, Sala de Casación Penal. (2014). *Sentencia SP13290 del 1 de octubre de 2014.* M. P.: María del Rosario González Muñoz.

Corte Suprema de Justicia, Sala de Casación Penal. (2022). *Sentencia SP2699 del 3 de agosto de 2022 (Rad. 59733).* M. P.: Fernando León Bolaños Palacios.

Corte Suprema de Justicia, Sala de Casación Penal. (2023). *Sentencia SP-055* del 22 de febrero de 2023. M. P.: Myriam Ávila Roldán.

Jurisprudencia internacional y lineamientos internacionales.

Comisión Interamericana de Derechos Humanos (CIDH). (2018). *Derechos humanos y seguridad digital: una pareja perfecta.* OEA.

Consejo de Derechos Humanos. (2012). *Resolución A/HRC/20/L.13: Promoción, protección y disfrute de los derechos humanos en Internet.* Naciones Unidas.

Consejo de Seguridad de las Naciones Unidas. (2021). *Tecnologías de la información y las comunicaciones.* Comité contra el Terrorismo, Dirección Ejecutiva del Comité contra el Terrorismo (CTED). Recuperado de https://www.un.org/securitycouncil/ctc/content/information-and-communications-technologies

Foro Económico Mundial (FEM). (2018). *Our Shared Digital Future: Building an inclusive, trustworthy and sustainable digital society.* Recuperado de http://www3.weforum.org/docs/WEF_Our_Shared_Digital_Future_Report_2018.pdf

INTERPOL. (2021). *Guía nacional de estrategias contra el ciberdelito.* Recuperado de https://www.interpol.int/en/Crimes/Cybercrime

Instituto Interregional de las Naciones Unidas para Investigaciones sobre la Delincuencia y la Justicia (UNICRI). (2020). *Detener el virus de la desinformación: El riesgo del uso malicioso de las redes sociales durante la COVID-19 y las opciones tecnológicas para combatirlo.* Naciones Unidas.

Naciones Unidas. (1949). *Convenios de Ginebra del 12 de agosto de 1949.* Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos (ACNUDH).

Naciones Unidas. (1977a). *Protocolo adicional I a los Convenios de Ginebra del 12 de agosto de 1949 relativo a la protección de las víctimas de los conflictos armados internacionales.* ACNUDH.

Naciones Unidas. (1977b). *Protocolo adicional II a los Convenios de Ginebra del 12 de agosto de 1949 relativo a la protección de las víctimas de los conflictos armados sin carácter internacional.* ACNUDH.

Naciones Unidas. (1994). *Medidas para eliminar el terrorismo internacional (Resolución 49/60).* Asamblea General de las Naciones Unidas, 9 de diciembre de 1994. https://undocs.org/es/A/RES/49/60

Oficina de las Naciones Unidas contra la Droga y el Delito. (2018). *El marco jurídico universal contra el terrorismo: Plan de estudios para la capacitación jurídica contra el terrorismo.* Naciones Unidas. Recuperado de https://www.unodc.org/documents/terrorism/Publications/Module%202/Module_2_Spanish.pdf

Organización de los Estados Americanos (OEA). (2003). *Declaración sobre Seguridad en las Américas.* Conferencia Especial sobre Seguridad, Ciudad de México, 28 de octubre de 2003.

Organización de los Estados Americanos (OEA). (2004). *Estrategia Interamericana Integral de Seguridad Cibernética.* Resolución AG/RES. (XXXIV-O/04).

Tribunal de Justicia de la Unión Europea (TJUE). (2014). *Digital Rights Ireland Ltd contra Minister for Communications, Marine and Natural Resources y otros (C-293/12).* Informes del Tribunal de Justicia de la Unión Europea.

Tribunal de Justicia de la Unión Europea (TJUE). (2015). *Maximillian Schrems contra Data Protection Commissioner (C-362/14).* Informes del Tribunal de Justicia de la Unión Europea.

Tribunal de Justicia de la Unión Europea (TJUE). (2020). *Data Protection Commissioner contra Facebook Ireland Ltd y Maximillian Schrems (C-311/18).* Informes del Tribunal de Justicia de la Unión Europea.

Tribunal Europeo de Derechos Humanos (TEDH). (2008). *K.U. contra Finlandia (Solicitud núm. 2872/02).* Base de datos HUDOC. Disponible en https://hudoc.echr.coe.int

Tribunal Europeo de Derechos Humanos (TEDH). (2020). *Buturugă contra Rumanía (Solicitud núm. 56867/15).* Base de datos HUDOC. Disponible en https://hudoc.echr.coe.int

Tribunal Europeo de Derechos Humanos (TEDH). (2021). *Big Brother Watch y otros contra Reino Unido (Solicitudes núm. 58170/13, 62322/14 y 24960/15).* Base de datos HUDOC. Disponible en https://hudoc.echr.coe.int

Acuerdos Institucionales.

Consejo Académico de la Universidad Colegio Mayor de Cundinamarca. (2022, 10 de octubre). *Acuerdo 069 de 2022: Por el cual se actualizan las Líneas Institucionales de Investigación para la Universidad Colegio Mayor de Cundinamarca.* Recuperado de https://www.unicolmayor.edu.co/universidad/normatividad/consejo-academico/acuerdos/acuerdos-2022/acuerdo-69-2022

Bibliografía

Agudelo, N. (2014). Estudio preliminar: La actualidad del pensamiento de Beccaria. En N. Agudelo (Coord.), *De los delitos y de las penas: Edición 250 años* (p. 24). Medellín: Ediciones Nuevo Foro.

Alexy, R. (2004). *Teoría de los derechos fundamentales* (E. Garzón Valdés, Trad.). Madrid: Centro de Estudios Constitucionales.

Alfredo Fontana, I., Zechlinski dos Santos, L., & Fonseca Ferreira, R. (2024). El fenómeno digital, el poder de los gigantes tecnológicos y los desafíos regulatorios en Brasil. *Revista Misión Jurídica, 17*(27), 31–?

Almeyda Velásquez, D. A. (2015). *Bases para la contención del Derecho Penal del Enemigo: Dialéctica de la interpretación y delito de afiliación a organización terrorista* [Tesis de maestría, Universidad Nacional Mayor de San Marcos]. Lima, Perú.

Ambos, K. (2007). *Derecho Penal del enemigo.* Universidad Externado de Colombia.

Andrade Becerra, O. D. (2014). *Conceptualización del terrorismo en Colombia (1978–2010)* [Tesis doctoral].

Ara Pinilla, I. (2000). *El principio de igualdad.* Madrid: Dykinson.

Aramburú, I. J. M. (2015). Los enemigos de Jakobs. *Revista Pensamiento Penal.* https://www.pensamientopenal.com.ar/doctrina/40722-enemigos-jakobs

Aranzamendi, L. (2015). *Investigación jurídica* (2.ª ed.). Lima, Perú: Editorial Jurídica Grijley.

Arias Eibe, M. J. (2006). Funcionalismo penal moderado o teleológico-valorativo versus funcionalismo normativo o radical. *Doxa: Cuadernos de Filosofía del Derecho,* (29), 439–453.

Arias Eibe, M. J. (2017). *Bases sociológicas del funcionalismo penal contemporáneo* [Artículo académico]. Universidad de Santiago de Compostela. https://perso.unifr.ch/derechopenal/assets/files/articulos/a_20080521_18.pdf

Asamblea General de las Naciones Unidas. (1994). *Medidas para eliminar el terrorismo internacional (Resolución 49/60, A/RES/49/60).* Naciones Unidas.

Barlow, J. P. (1996). *A declaration of the independence of cyberspace.* Electronic Frontier Foundation. https://www.eff.org/cyberspace-independence

Bautista García, F. (2020). *Incidencia del COVID-19 en el cibercrimen del 2020 y futuros retos.* UNODC, Colombia.

Beck, U. (1986). *La sociedad del riesgo: Hacia una nueva modernidad.* Paidós.

Bermúdez Bueno, W., & Morales Manzur, J. C. (2012). Estado Social de Derecho: Consideraciones sobre su trayectoria histórica en Colombia a partir de 1991. *Cuestiones Políticas, 28*(48), 51–77.

Bravo Peña, N. A. (2007). *Derecho Penal del enemigo: ¿Evolución o primitivismo del Derecho Penal?* [Memoria de licenciatura, Universidad de Chile].

Cabrera Suárez, L. A. (2018). El significado real de que Colombia sea un Estado Social de Derecho. *DIXI, 20*(27), 1–20. https://doi.org/10.16925/di.v20i27.2390

Camps, V. (2017). *Breve historia de la ética.* RBA Libros.

Cárdenas Bonilla, W. A. (2012). *Una nueva mirada a la expansión del Derecho Penal* [Artículo académico]. Universidad de los Andes.

Cardeño, J. I. C. (2021). *Sociedad digital en Latinoamérica 2020–2021: Un futuro posible de Colombia como sociedad digital* (p. 321). Technical University of Denmark. https://local.forskningsportal.dk/local/dki-cgi/ws/cris-link?src=aau&id=aau-349bf1c3-c019-47ea-8515-944bd1595c3a

Castells, M. (2009). *La era de la información: Economía, sociedad y cultura. Vol. I: La sociedad red* (2.ª ed.). Madrid: Alianza Editorial.

Chaliand, G., & Blin, A. (Eds.). (2017). *Historia del terrorismo: De la Antigüedad a Al Qaeda* (F. D'Eça Leal, Trad.). SAJ/INF.

Cote-Barco, G. E. (2008). Constitucionalización del Derecho Penal y proporcionalidad de la pena. *Vniversitas,* (116), 119–151.

Delgado Parra, C. (2011). El criterio amigo/enemigo en Carl Schmitt: el concepto de lo político como una noción ubicua y desterritorializada. *Cuaderno de materiales, 23,* 175–183. Recuperado de https://www.filosofia.net/materiales/pdf23/CDM11.pdf

Denning, D. E. (2000). *Cyberterrorism.* Disponible en http://www.cs.georgetown.edu/~denning/ (Consultado el 15.06.2015).

El Espectador. (2025). Riesgos en línea: 78% de los colombianos ha sido víctima de amenazas digitales. *El Espectador.* Recuperado de https://www.elespectador.com/tecnologia/riesgos-en-linea-78-de-los-colombianos-ha-sido-victima-de-amenazas-digitales/

Fernández Carrasquilla, J. (2006). *Derecho Penal liberal de hoy.* Bogotá: Editorial Gustavo Ibáñez.

Ferrajoli, L. (1995). *Derecho y razón: Teoría del garantismo penal.* Madrid: Trotta.

Ferrajoli, L. (2001). *Derecho y razón: Teoría del garantismo penal.* Madrid: Trotta.

Ferrajoli, L. (2004). *Derecho y razón: Teoría del garantismo penal* (6.ª ed.). Madrid: Trotta.

Ferrajoli, L. (2006). *Garantismo penal.* UNAM, Instituto de Investigaciones Jurídicas (Serie Estudios Jurídicos, No. 34).

Francisco Agra, S. V. (2022). La digitalización del miedo: del terrorismo "clásico" al terrorismo "tecnológico". *El Criminalista Digital. Papeles de Criminología,* (10), 17–37.

Foucault, M. (2007). *Seguridad, territorio, población: Conferencias en el Collège de France 1977–1978* (G. Burchell, Ed. y Trad.). Palgrave Macmillan.

Fundación Paz y Reconciliación (PARES). (2022). *La ciberseguridad después de la pandemia: una mirada a los delitos informáticos en Colombia.* Línea de Convivencia y Seguridad Ciudadana. Colombia.

García Amado, J. A. (2006). El obediente, el enemigo, el Derecho Penal y Jakobs. *Nuevo Foro Penal,* 69, 100.

Gialdino, M. R. (2018). *Abordando la seguridad pública desde la Filosofía del Derecho.*

Gómez Mena, C., & Cifuentes Castaño, M. (2011). *Derecho Penal del enemigo.* Universidad Libre. Colombia. Recuperado de https://hdl.handle.net/10901/16735

González Monguí, P. E. (2019). La negación de la calidad de ciudadano o de persona en el Derecho Penal del enemigo. *Opción, 35*(Especial 25), 1070–1103.

Gordillo Álvarez-Valdés, M. V. (1985). El problema de la relación entre teoría y práctica en educación según el pensamiento alemán contemporáneo. *Revista Española de Pedagogía, 43*(167), 5–22.

Grabosky, P. (2001). Criminalidad virtual: Viejo vino en botellas nuevas. *Social & Legal Studies, 10*(2), 243–249. https://doi.org/10.1177/096466390101000204

Gracia Martín, L. (2005). Consideraciones críticas sobre el actualmente denominado Derecho Penal del enemigo. *Revista Peruana de Ciencias Penales,* 16, 371–420.

Habermas, J. (1981). *Teoría de la acción comunicativa.* Madrid: Taurus.

Hassemer, W. (1991). *Persona, mundo y responsabilidad: Bases para una teoría de la imputación en Derecho Penal.* Bogotá: Universidad Externado de Colombia.

Hernández Sampieri, R., Fernández Collado, C., & Baptista Lucio, P. (2014). *Metodología de la investigación* (6.ª ed.). McGraw-Hill Education.

Hobbes, T. (1993). *El ciudadano* (J. Rodríguez Feo, Trad.). Madrid: Debate.

Hobbes, T. (1994). *Leviatán o la materia, forma y poder de una república eclesiástica y civil* (M. Sánchez Sarto, Trad.). México: Fondo de Cultura Económica.

Hobbes, T. (2019). *Leviatán* (A. Padrón Alfonso, Trad.). Madrid: Editorial Verbum. (Obra original publicada en 1651).

Home Office. (2013). *Ciberdelito: Una revisión de la evidencia.* United Kingdom Government. https://www.gov.uk/government/publications/cyber-crime-a-review-of-the-evidence

Iftikhar, S. (2024). El ciberterrorismo como amenaza global: una revisión sobre sus repercusiones y contramedidas. *PeerJ Computer Science, 10*, 1772. https://doi.org/10.7717/peerj-cs.1772

Izuzquiza, I. (1989). *La sociedad sin hombres: Niklas Luhmann o la teoría como escándalo.* Barcelona: Anthropos.

Jakobs, G. (1985). Criminalización en el estadio previo a la lesión de un bien jurídico [Conferencia]. Frankfurt am Main, Alemania.

Jakobs, G. (1996). *Sociedad, norma y persona en la teoría de un Derecho Penal funcional.* Bogotá: Universidad Externado de Colombia.

Jakobs, G. (2003). Derecho Penal del ciudadano y Derecho Penal del enemigo. En Jakobs/Cancio, *Derecho Penal del enemigo* (M. Cancio Meliá, Trad.). Madrid: Thomson Civitas.

Jakobs, G. (2004). Personalidad y exclusión en Derecho Penal. En Q. López Barja de (Comp.), *Dogmática de Derecho Penal y configuración normativa de la sociedad* (pp. 51–73). Madrid: Thomson Civitas.

Jakobs, G. (2006a). Derecho Penal del ciudadano y Derecho Penal enemigo. En Jakobs/Cancio, *Derecho Penal del enemigo* (2.ª ed.; M. Cancio Meliá, Trad.). Madrid: Thomson Civitas.

Jakobs, G. (2006b). ¿Terroristas como personas en Derecho? En Jakobs/Cancio, *Derecho Penal del enemigo* (2.ª ed.; M. Cancio Meliá, Trad.). Madrid: Thomson Civitas.

Jakobs, G. (2006c). El terrorismo internacional se puede combatir con el Derecho Penal del enemigo (entrevista, Bogotá, 1 de junio de 2006). *Revista Peruana de Doctrina y Jurisprudencia Penales,* 7, 613–617.

Jakobs, G. (2007a). La imputación jurídico-penal y las condiciones de la vigencia de la norma. En C. Gómez-Jara Diez (Coord.), *Teoría de los Sistemas y Derecho Penal* (pp. 225–248). Lima: ARA Editores.

Jakobs, G. (2007b). ¿Derecho Penal del enemigo? Un estudio acerca de los presupuestos de la juridicidad. En Jakobs/Polaino Navarrete, *Las condiciones de juridicidad del sistema penal* (pp. 17–44). Lima: Editorial Grijley.

Johnson, D. R., & Post, D. (1996). Law and borders: The rise of law in cyberspace. *Stanford Law Review*, *48*(5), 1367–1402. https://doi.org/10.2307/1229390

Jones-Chaljub, S. (2022). El ciberespacio como un entorno de interacciones. En S. Jones-Chaljub, *Conceptualización del ciberespacio humano* (pp. 17–18). ESDEG. https://doi.org/10.25062/9786287602137.01

Llinares, F. M. (2021). Crimen, cibercrimen y COVID-19. *IDP Revista de Internet, Derecho y Política*, 32. https://doi.org/10.7238/idp.v0i32.373815

Lopez, Z. (2001). El hombre frente al Derecho Penal en un Estado Social de Derecho (ESD). *Revista de Derecho,* (16II).

Mayer-Schönberger, V., & Cukier, K. (2013). *Big data: A revolution that will transform how we live, work, and think.* Houghton Mifflin Harcourt.

Mendieta, D., & Tobón, M. L. (2018). La dignidad humana como fundamento del Estado social y democrático de derecho: una mirada desde el caso colombiano. *RECHTD, 10*(3), 278–289. https://doi.org/10.4013/rechtd.2018.103.05

Mendoza Buergo, B. (2001). *El Derecho Penal del enemigo: Análisis y crítica.* Madrid: Civitas.

Mesa C. W. A. (2022). La rebelión y el terrorismo en sede judicial: hacia una comprensión de la estrategia de ruptura judicial. *Revista de la Facultad de Derecho de México, 72*(283), 119–148.

Montero, E. (2008). *El funcionalismo penal, una introducción a la teoría de Günther Jakobs.* Trujillo.

Montoro Ballesteros, A. (2007). El funcionalismo en el Derecho. *Anuario de Derechos Humanos: Nueva Época*, 8, 365–374.

Muñoz Sánchez, O., Pontvianne, J., & Álvarez Posada, S. (2019). El terrorismo en el escenario del post-acuerdo en Colombia. *Revista de Estudios en Seguridad Internacional*, *5*(1), 83–100. https://doi.org/10.18847/1.9.7

Nieves Sanz. (2019). *Política criminal.* Editorial Ratio Legis.

Parma, C. (2009). *Roxin o Jakobs: ¿Quién es el enemigo en el Derecho Penal?* Ediciones Jurídicas Andrés Morales.

Pereira, R., Souza, C. M. de, & Cimolin, B. C. (2021). La responsabilidad penal del infractor de medida de salud preventiva: aproximación a la teoría de Günther Jakobs. *Misión Jurídica, 14*(21). https://doi.org/10.25058/1794600X.1888

Piñón, L. C., Sapién, A. L., & Gutiérrez, M. del C. (2023). Capacitación en ciberseguridad en una empresa mexicana. *Información Tecnológica, 34*(6), 43. https://doi.org/10.4067/S0718-07642023000600043

Polaino-Orts, M. (2012). Dogmática penal y libertad. En *Derecho Penal como sistema de autodeterminación personal* (pp. 19–37). Lima: ARA Editores.

Poveda Criado, M. Á., & Torrente Barredo, B. (2016). Redes sociales y ciberterrorismo. : Las TIC como herramienta terrorista. *Opción, 32*(8), 509–518. https://www.redalyc.org/pdf/310/31048481030.pdf

Rapoport, D. C. (2004). Las cuatro oleadas del terrorismo moderno. En *I Jornada sobre terrorismos en el siglo XXI* (pp. 1–12). Fundación Manuel Giménez Abad.

Real Academia Española. (2024). *Neutralizar.* En *Diccionario de la lengua española* (23.ª ed.). Recuperado de https://dle.rae.es/neutralizar

Rincón Romero, L. M. (2016). La permeabilización del derecho por los medios de comunicación: La incursión del Derecho Penal del enemigo. *Misión Jurídica, 11,* 303–325.

Rodríguez Jiménez, A., & Pérez Jacinto, A. O. (2017). Métodos científicos de indagación y de construcción del conocimiento. Revista Escuela de Administración de Negocios. *Revista EAN*, (82), 1–26.

Roxin, C. (1997). *Política criminal y sistema del Derecho Penal* (J. Bustos Ramírez, Trad.). Madrid: Civitas. (Obra original publicada en 1963).

Saidiza Peñuela, H. F., & Carvajal Martínez, J. E. (2016). Crisis del Estado de derecho en Colombia: un análisis desde la perspectiva de la legislación penal. *IUSTA*, (44), 17–39.

Sain, G. (2018). La estrategia gubernamental frente al cibercrimen:la importancia de las políticas preventivas más allá de la solución penal. En R. A. Parada & J. D. Errecaborde (Comps.), *Cibercrimen y delitos informáticos* (pp. 7–33). Buenos Aires: Erreius.

Sánchez, H. N., Peña, M. P. C., Sierra-Zamora, P. A., & Bermúdez-Tapia, M. (2024). El ciberterrorismo en la legislación colombiana: un análisis desde la criminología. *The Law, State and Telecommunications Review*, *16*(1), 344–364.

Sánchez González, A. (2009). Luhmann, Jakobs y el Derecho Penal del enemigo. *Revista Crítica Jurídica,* (28), 1–20.

Silva Sánchez, J.-M. (2001). *La expansión del Derecho Penal: Aspectos de la política criminal en las sociedades postindustriales* (2.ª ed.). Madrid: Civitas.

Solano de Jinete, N., & Sepúlveda López, M. (2008). *Metodología de la investigación social y jurídica* (1.ª ed.). Grupo Editorial Ibáñez.

Spaemann, R. (1989). *Lo natural y lo racional* (D. Innerarity & J. Olmo, Trads.). Madrid: Rialp.

Tapia Hernández, E. F., Ruíz Canizales, R., & Vega Páez, A. (2021). La importancia de la ciberseguridad y los derechos humanos en el entorno virtual. *Revista Misión Jurídica, 14*(20), 142–158. https://doi.org/10.25058/1794600X.1912

Theohary, C. A., & Rollins, J. W. (2015). *Ciberguerra y ciberterrorismo: En resumen* (Informe No. R43955). Congressional Research Service. https://sgp.fas.org/crs/natsec/R43955.pdf

Thomas, T. L. (2003). Al Qaeda y el internet: El peligro de la “ciberplanificación”. *Parameters, 33*(1), 112–123.

Torres Vásquez, H. (2015). Conflicto armado y terrorismo en Colombia. El terrorismo de las Farc-EP de acuerdo con la jurisprudencia de la Corte Constitucional colombiana. *Iustitia, 13*, 11–34.

Torres Vásquez, H., Tirado Acero, M., & Trujillo Florián, S. (2018). Funcionalismo radical penal a partir de la bioética. *Revista Republicana, 25*, 179–198. https://doi.org/10.21017/Rev.Repub.2018.v25.a55

Tuset Varela, D. (2024). El derecho de la inteligencia artificial desde la perspectiva de Michel Foucault: Biopoder, vigilancia y reconfiguración de la normatividad jurídica. *Journal of Social Sciences.* https://doi.org/10.4236/jss.2024.1212012

Vázquez Pérez, E. D. (2022). La representación de la sociedad en el funcionalismo normativista de Günther Jakobs. Disenso. Crítica y Reflexión Latinoamericana. *Disenso, 5*(II), 1–6.

Wall, D. S. (2007). *Ciberdelito: La transformación del crimen en la era de la información.* Polity Press.

Weimann, G. (2006). *Terrorismo en Internet: La nueva arena, los nuevos desafíos.* United States Institute of Peace Press.

Yar, M. (2006). *Cybercrime and society.* London: Sage.

Zaffaroni, E. R. (2006). *Derecho Penal: Parte general.* Buenos Aires: Ediar.

Zaffaroni, E. R. (2011a). *El enemigo en el Derecho Penal.* Coyoacán.

Zaffaroni, E. R. (2011b). Estado y seguridad pública: algunas consideraciones básicas. Recuperado de http://www.minseg.gob.ar/estado-y-seguridad-publica-algunas-consideraciones-basicas

Zeiger, S., & Gyte, J. (2020). The role of internet and social media use in radicalization processes. En *Extremism and online radicalization.* Hedayah Center.

Zuboff, S. (2019). *La era del capitalismo de la vigilancia.* Paidós.

Bibliografía complementaria

Álvarez Cozzi, C. (2016). La asistencia penal internacional y la extradición en delitos de narcotráfico, lavado de activos y financiación del terrorismo y corrupción internacional. *Misión Jurídica, 9*(10), 77–91. https://doi.org/10.25058/1794600X.118

Cancio Meliá, M. (2006). ¿De nuevo: "Derecho Penal" del enemigo? *Revista Penal,* (17), 67–87.

Cutrale, E. (2020). Terrorismo y Derecho Penal: Del Derecho Penal de última ratio al Derecho Penal del enemigo. *Universitas,* (31), 89–107. https://doi.org/10.20318/universitas.2020.5139

De Jinete, N. S., & Serrano, O. H. (2012). Recompensas: una incongruencia de orden filosófico social y jurídico, en un Estado Social de Derecho como el que se predica en Colombia. *Misión Jurídica, 5*(5), 241–265.

Ferrajoli, L. (2006). El Derecho Penal del enemigo y la disolución del Derecho Penal. *Sistema Penal & Violencia, 1*(1), 5–25.

Muñoz, J. R. A. (2012). La participación en el Estado social y democrático de Derecho. *A&C-Revista de Direito Administrativo & Constitucional, 12*(48), 13–40.

Polaino-Orts, M. (2011). ¿Cómo combate el Estado de Derecho el terrorismo? En Jakobs/Polaino-Orts, *Persona y enemigo* (pp. 83–125). Lima: ARA.

Urquizo Olaechea, J. (2007). Derecho Penal del enemigo. *Revista de Derecho y Ciencia Política*, 64(1–2), 229–260.

Velásquez V., F. (2004). Globalización y Derecho Penal. En M. Losano & F. Muñoz Conde (Coords.), *El Derecho ante la globalización y el terrorismo* (pp. 185–208). Valencia: Tirant lo Blanch.

Woloszyn, A. L. (2024). El crimen del terrorismo: una hipótesis psicoanalítica. *Misión Jurídica, 17*(27), 65–79. https://doi.org/10.25058/1794600X.2458

DERECHO EN NUESTRA U

Maestría en Derecho Penal: Terrorismo Digital en Colombia

Martes 2 de septiembre | 10:00 a.m.

UNIVERSIDAD COLEGIO MAYOR DE CUNDINAMARCA

Acreditación Institucional de ALTA CALIDAD

SEÑAL MAYOR

KAROL VALENTINA CHAVES PRIETO <kchaves@universidadmayor.edu.co>

Remisión de artículo para consideración y posible publicación

Revista Misión Jurídica - UCMC - <misionjuridica@universidadmayor.edu.co> 4 de diciembre de 2025 a las 9:13

Para: KAROL VALENTINA CHAVES PRIETO <kchaves@universidadmayor.edu.co>
Cc: cotidianocreativo@gmail.com, orsobar@hotmail.com, Myriam Sepulveda López <myriam.sepulveda@universidadmayor.edu.co>, Claudia Patricia Orduz Barreto <corduz@universidadmayor.edu.co>

Estimadas autoras, reciban un cordial saludo.
En primer lugar agradecemos profundamente por el envío de su trabajo de investigación para surtir el proceso de publicación en Misión Jurídica.
Informamos que estamos revisando su artículo para observaciones previas a su paso a evaluadores. De existir estaremos comunicandonos esta semana y luego será enviado a evaluadores.
Muchas gracias por la confianza en nuestra revista.
Cordialmente,
Equipo editorial
Misión Jurídica

[El texto citado está oculto]

> [El texto citado está oculto]
> ---
> **AVISO LEGAL**

AVISO LEGAL

KAROL VALENTINA CHAVES PRIETO <kchaves@universidadmayor.edu.co>

Remisión de artículo para consideración y posible publicación

KAROL VALENTINA CHAVES PRIETO <kchaves@universidadmayor.edu.co> 3 de diciembre de 2025 a las 14:53

Para: Revista Misión Jurídica - UCMC - <misionjuridica@universidadmayor.edu.co>, cotidianocreativo@gmail.com, orsobar@hotmail.com
Cc: Myriam Sepulveda López <myriam.sepulveda@universidadmayor.edu.co>, Claudia Patricia Orduz Barreto <corduz@universidadmayor.edu.co>

Señores

Revista Misión Jurídica
Comité Editorial
Bogotá DC.

Reciban un cordial saludo.

Por medio del presente nos permitimos remitir para su consideración el artículo titulado El Terrorismo Digital en Colombia: entre el Derecho Penal del Enemigo y el Estado Social de Derecho.“”, el cual constituye un artículo de resultados derivado de la investigación desarrollada en el marco de la tesis de maestría de Derecho Penal , asociada al proyecto de investigación “Terrorismo Digital en Colombia: Un análisis desde el Derecho Penal del Enemigo, 2020-2025, adscrito a la Universidad Colegio Mayor de Cundinamarca.

En el manuscrito se abordan analiza el tratamiento jurídico-penal del Terrorismo Digital en Colombia entre 2020 y 2025, a la luz de los fundamentos del Derecho Penal del Enemigo formulado por Günther Jakobs; con el propósito de determinar si la respuesta estatal frente a las amenazas del ciberespacio ha mantenido su anclaje en el Estado Social de Derecho o si ha derivado hacia un modelo punitivo de excepción, con el propósito de contribuir a la discusión académica y jurídica, en coherencia con las líneas temáticas y el enfoque crítico de la revista.

Manifestamos que el artículo es original e inédito, no ha sido publicado previamente ni se encuentra en evaluación simultánea en otra revista.

Asimismo, quedamos atentos/as a sus comentarios, observaciones y a cualquier requerimiento adicional que estimen pertinente para fortalecer el manuscrito dentro del proceso editorial.

Agradecemos de antemano su atención y la evaluación del texto para eventual publicación en *Misión Jurídica*.

Cordialmente,

Karol Valentina Chaves Prieto.

Dra. Claudia Patricia Orduz Barreto

Dra. Myriam Sepúlveda Lopez.

Articulo El Terrorismo Digital en Colombia .docx
274K

El Terrorismo Digital en Colombia: entre el Derecho Penal del Enemigo y el Estado Social de Derecho.*

Karol Valentina Chaves Prieto kchaves@universidadmayor.edu.co [*]

Myriam Sepúlveda López myriam.sepulveda@universidadmayor.edu.co**

Dra. Claudia Patricia Orduz Barreto corduz@universidadmayor.edu.co***

RESUMEN.

La presente investigación analiza el tratamiento jurídico-penal del Terrorismo Digital en Colombia entre 2020 y 2025, a la luz de los fundamentos del Derecho Penal del Enemigo formulado por Günther Jakobs; con el propósito de determinar si la respuesta estatal frente a las amenazas del ciberespacio ha mantenido su anclaje en el Estado Social de Derecho o si ha derivado hacia un modelo punitivo de excepción.

El estudio parte de la comprensión del impacto de las transformaciones tecnológicas sobre el derecho penal y de cómo el terrorismo ha trasladado su escenario de acción al entorno digital,

---

* Artículo que presenta resultados de un proyecto de investigación terminado denominado Terrorismo Digital (TDig) en Colombia: Un análisis desde el derecho penal del enemigo, 2020-2025- Universidad Colegio Mayor de Cundinamarca. Bogotá D.C.

*Abogada egresada de la Universidad Colegio Mayor de Cundinamarca, con formación en derecho público y derechos humanos. Especialista en Derecho Internacional Público con énfasis en Derechos Humanos y aspirante a Magister en Derecho Penal de la misma universidad.

**Trabajadora Social de Universidad Colegio Mayor de Cundinamarca, Abogada Universidad La Gran Colombia, Especialista en docencia Universidad Santo Tomas, Especialista en Derecho de Familia Universidad Nacional de Colombia, Magister en Pedagogía de la Universidad Pedagógica y Tecnológica de Colombia, Magister en Derecho Administrativo de Universidad Libre, Doctora en Filosofía Jurídica de la Universidad Nacional de Educación a Distancia de Madrid -España (UNED), Posdoctorado en educación de Universidad Santo Tomas, docente investigadora líder del grupo Pedagogía y Derecho, coordinadora Semillero Pedagogía y Derecho.

*** Abogada, especialista en Derecho Penal y Criminología, Magister en Derecho Penal, con amplia trayectoria laboral en el sector público, (ocupando cargos como Juez de Ejecución de penas y medidas de seguridad, Juez Penal del Circuito bajo el sistema ley 600 de 2000 y Juez Penal del Circuito de Conocimiento en el actual sistema penal con tendencia acusatoria Ley 906 de 2004). y privado (como asesora jurídica y abogada litigante). Experiencia en el sector universitario como directivo, docente, conferencista e investigadora en las áreas de derechos humanos, derecho penal, criminología y política criminal en programas de pregrado y posgrado. Doctorado en Derecho Universidad de Salamanca y conciliadora en Derecho.

aprovechando la desregulación y la expansión del uso de internet, especialmente tras la pandemia de la COVID-19.

PALABRAS CLAVE:

Terrorismo Digital, Derecho Penal del Enemigo, Estado Social de Derecho, Seguridad Digital, y Ciberespacio.

ABSTRACT

This research analyzes the legal and criminal treatment of digital terrorism in Colombia between 2020 and 2025, in light of the foundations of Enemy Criminal Law (TDPE) formulated by Günther Jakobs, with the aim of determining whether the state's response to cyberspace threats has remained anchored in the Social Rule of Law or has shifted toward an exceptional punitive model.

The study begins with an understanding of the impact of technological transformations on criminal law and of how terrorism has shifted its arena of action to the digital environment, taking advantage of deregulation and the expansion of internet use, especially since the COVID-19 pandemic.

Keywords: Digital terrorism, enemy criminal law, social rule of law, digital security, and cyberspace.

INTRODUCCIÓN

Con el desarrollo tecnológico, la sociedad ha evolucionado de manera significativa transformando las dinámicas que de ella se desprenden, particularmente, al generar nuevos espacios de conexión no físicos, como lo es el ciberespacio donde se ha concentrado el uso exponencial de la tecnologías dedicadas a la información y/o comunicación, también llamadas (TIC), convirtiéndose tanto en una oportunidad de avance, como una nueva amenaza que desafía los marcos jurídicos tradicionales bajo un mundo dirigido por alcances globalizados.

En este contexto, las nuevas tecnologías informáticas que procesan de manera eficiente grandes cantidades de información, han sido acaparadas por personas dispuestas actuar en contra de los propios fines de la población, facilitando y mutando la comisión de conductas punibles de manera inclemente, siendo previsible la respuesta punitiva del Estado.

En verbigracia, el terrorismo como figura tradicional de violencia, que parte como actuación criminal en contra de los intereses de la sociedad ha descubierto en estos espacios virtuales poco regularizados, una forma eficaz de ejercer su actividad, obteniendo provecho al rol emergente de la tecnología para la masterización de sus actos.

Colombia, no ha sido indiferente a esta tendencia, la seguridad digital para el territorio se ha convertido en un objetivo trascendental; dado a las lagunas jurídicas que han surgido frente a la rápida evolución del ciberespacio que actores terroristas han sabido aprovechar, intensificando sus operaciones a partir de la pandemia de COVID 19, al existir una mayor dependencia a la tecnología.

Ante este contexto, el Terrorismo Digital (TDig) se presenta como una amenaza latente para el sistema social, acelerado por una pandemia; que en particular, compromete la estabilidad del orden social y la seguridad nacional al generar miedo y zozobra en la población en el ciberespacio y comprometiendo la integridad informacional de las instituciones de los Estados.

Frente a ello, surge la necesidad de abordar como el Estado ha fortalecido su respuesta, frente a este problema, y si en su camino ha endurecido la legislación penal o ha generado estrategias públicas de persecución digital como los documentos CONPES 3995 de 2020 la "Política Nacional de Seguridad Digital" y 4144 de 2025 "Política Nacional de Inteligencia Artificial".

Así, se pone en consideración reflexionar si las medidas contenidas en tales políticas encauzadas a garantizar la seguridad digital y evitar el riesgo indeseable de los riesgos tecnológicos

acaban por introducir una perspectiva de control que, inevitablemente, reemplace el derecho penal tradicional.

Continuando con este razonamiento, la expansión del aparato punitivo en las esferas del ciberespacio, junto a la retórica de la seguridad, puede suponer, por el contrario, un tránsito del derecho penal garantista a un derecho penal preventivo y de excepción, donde el sospechoso ciudadano se convierte en "enemigo" incluso antes de haber perpetrado una conducta punible.

Por ello, se pretende analizar ¿De qué manera se ha desarrollado el Terrorismo Digital (TDig) en Colombia en relación con los fundamentos teóricos del Derecho Penal del Enemigo (DPE) de Günter Jakobs entre 2020 a 2025?

Partiendo de la posibilidad de que el Estado Colombiano frente al Terrorismo Digital (TDig) se encuentre incorporando —de manera implícita o parcial— los postulados de este derecho excepcional.

En suma, resulta significativo y necesario este trabajo al examinar un fenómeno jurídico como el Terrorismo Digital (TDig) inexplorado desde una óptica crítica, interdisciplinaria y constitucional, con la que se puede aportar claridad sobre los problemas que presenta el Estado colombiano frente a la criminalidad digital.

En definitiva, la investigación tiene por objeto ultimo contribuir al fortalecimiento de un modelo de Derecho Penal garantista, contra la lucha contra el Terrorismo Digital (TDig), el cual debe ser desarrollado dentro del ordenamiento jurídico y no al margen de este.

METODOLOGÍA.

La ruta metodológica propuesta en el presente artículo de reflexión, se edifica en una estructura de carácter jurídico - analítico, cuyo enfoque es eminentemente cualitativo; por cuanto, "insiste en la relevancia del fenómeno frente al rigor e intenta comprender la realidad dentro de un contexto dado" (Solano & Sepúlveda, 2008, p. 32).

En este caso, se encuentra orientado a examinar desde la hermenéutica el fenómeno del Terrorismo Digital (TDig) y su tratamiento en el ordenamiento colombiano a la luz de los postulados de la Teoría del Derecho Penal del Enemigo (TDPE) de Günter Jakobs y sus tensiones con los principios del Estado Social de Derecho (ESD).

Lo anterior, por cuanto se permite examinar el fenómeno desde una perspectiva teórica y hermenéutica al desarrollar interpretación crítica de fuentes jurídicas, doctrinales, normativas y jurisprudenciales, sin recurrir a la recolección de datos cuantitativos, lo que posibilita la construcción de conocimiento interpretativo a partir de documentos legales y académicos

RESULTADOS

En la última década, el Terrorismo Digital (TDig) ha emergido como una amenaza creciente en Colombia, experimentando un notable auge a partir de la pandemia de COVID-19, planteando desafíos sin precedentes para la seguridad nacional, lo cual, ha sido objeto de análisis por parte de organismos internacionales. El Instituto de Investigación Interregional sobre Crimen y Justicia de las Naciones Unidas (UNICRI), en su informe de 2020, ha destacado:

> La desinformación y la información errónea en las redes sociales no son problemas nuevos, pero la crisis de la COVID-19 los ha amplificado y ha creado nuevas oportunidades para actores no estatales violentos. En los últimos meses hemos visto numerosos casos de uso malintencionado de las redes sociales, para socavar la confianza en los gobiernos y, al mismo tiempo, reforzar las narrativas extremistas y las estrategias de reclutamiento. (p.5).

A nivel nacional, el periódico el Espectador (2025) en su artículo establece que más del 78% ha sido víctima de amenazas digitales entre las principales se encuentran:

> (…) la desinformación (59 %), la exposición a contenidos violentos (47 %) y el discurso de odio (39 %). Además, el estudio alerta sobre un fenómeno preocupante: la creación de deepfakes de contenido pornográfico, una práctica que afecta al 20 % de los encuestados en Colombia, posicionando como el segundo país con mayor incidencia de este problema.

Estos datos reflejan, que los grupos terroristas han evolucionado para adaptarse a esta nueva era representando una mayor amenaza estatal en el anonimato, incitando la violencia, coordinando ataques, difundiendo discursos que afectan a la seguridad del Estado y sus ciudadanos, lo cual, demanda una respuesta eficaz ante las vulnerabilidades del ecosistema virtual.

Generalmente, la respuesta punitiva contempla nuevos desafíos dentro del marco del derecho penal tradicional, en la medida que su alcance puede resultar ineficiente ante la amenaza significativa que trasciende el cerco de criminalidad común y se concentra en un dominio artificial no físico.

En este escenario de la era digital, los Estados redefinen el concepto de seguridad tradicional, a un modelo de seguridad tecnológico y de riesgo, en el que la protección del orden social y de las informaciones en un pilar del poder estatal.

No obstante, como advierte Mendoza Buergo (2001),cuando derecho penal se orienta en función de control preventivo de un riesgo, se corre el peligro de convertir al ciudadano en objeto de la neutralización, alterando la balanza entre libertad y seguridad.

Por lo tanto, la Teoría del Derecho Penal del Enemigo (TDPE)tiene un sentido en la medida que ofrece una conceptualización que permite verificar si la contestación estatal frente al Terrorismo

Digital (TDig) se ajusta a un modelo de gestión del riesgo o a uno de neutralización del peligro, que amenaza los principios del Estado Social de Derecho (ESD).

Razón por la cual, la Teoría del Derecho Penal del Enemigo (TDPE) cumple con el papel de lente crítico, que permite examinar o escrutar si las políticas y normas que se adoptan respetan los límites constitucionales consentidos para el poder punitivo.

DESARROLLO DEL TRABAJO

En la actualidad, la tecnología ha cambiado la forma en cómo el ser humano percibe el mundo; ya que, el hombre impulsado por su necesidad de relacionarse en comunidad género herramientas comunicativas que trascienden sus propios alcances.

Entre ellas, destacan las redes de telecomunicaciones a nivel global, que constituye una compleja red de interconexiones de distinta naturaleza, donde se almacena una infinidad de datos de carácter informático, al permitir la continua comunicación entre personas, instituciones y sistemas automáticos.

De hecho, diversos autores como Mayer Schonberger, Kenneth Cukier (2013) e incluso Manuel Castells (2009) denominan este momento histórico como la "era del dato" o "la era del big data"; un periodo marcado por la producción, recolección, tratamiento, y circulación masiva de información personal, institucional y/o gubernamental, un fenómeno comparable a la Revolución Industrial.

No obstante, más allá de la mera utilidad funcional, quienes utilizan las telecomunicaciones han generado un nuevo ámbito social y político: el ciberespacio.

En el ciberespacio convergen múltiples redes de telecomunicaciones, que permiten la transmisión de datos en tiempo real, facilitando desde la interacción interpersonal hasta el

funcionamiento de complejos sistemas automatizados; sin embargo su conceptualización o delimitación es compleja por cuanto su definición continúa en construcción, al ser un fenómeno relativamente reciente y paradójicamente complejo.

Sin embargo, el ciberespacio es una zona sociotécnica, que permea todas las instancias de la vida social, emergiendo como la infraestructura para el tratamiento de datos informáticos por excelencia que en la actualidad es un pilar para la economía y la sociedad.

En esta nueva forma, los datos se convierten en un bien estratégico, capaz no sólo de generar valor económico, sino de adaptar o moldear comportamientos sociales, influir en decisiones políticas, y/o transformar relaciones de poder contemporáneo, al poseer, un componente virtual -en especial el internet y las redes sociales- el ciberespacio se edifica como una herramienta sofisticada de control social.

Bajo este marco de aceleración del término donde el componente virtual del ciberespacio -dibujado por redes sociales, aplicaciones, plataformas y flujos permanentes de datos- se consolida como un entorno de interacción y desarrollo, pero también como un espacio de alto riesgo. En respuesta, la seguridad digital se contrapone para garantizar la dignidad de los individuos en el desarrollo de su vida virtual.

La seguridad digital se erige como un componente esencial en una sociedad interconectada por las tecnologías de la información a nivel global. Su finalidad obra en la preservación del orden y estabilidad social en el ciberespacio mediante el accionar de los Estados, protegiendo los dominios digitales de sus conciudadanos, al ser una extensión de la intimidad del individuo en la que ejercen derechos fundamentales.

No obstante, a pesar de estas estrategias, la protección digital ha quedado mermada. Lo anterior, es porque al ser el ciberespacio una arquitectura abierta, descentralizada y, hasta cierto punto,

anónima, lo cual, genera un ámbito propenso a que varios actores no estatales hagan un uso estratégico, ideológico o criminal de este.

Con la crisis sanitaria y la globalización, las políticas desarrolladas comenzaron a tener lagunas en su actuar frente al nuevo panorama digital que se iba desarrollando, encontrando ausencia de una gobernanza jurídica tanto interna, como global, convirtiéndose en una amenaza más ofensiva para los Estados por las características que le son propias

Para Jorge Ivan Contreras Cardeño (2021) dispone que para la vigencia de 2020 "el impacto del COVID-19 supuso un nuevo acelerón en la digitalización de la sociedad, traducido en el crecimiento del uso de internet en general y de las redes sociales en particular" (p.102).

Con todo, la fragilidad estructural del espacio digital y la falta de una regulación global efectiva han sido ocupadas en la actualidad por aquellos que hacen un uso de la tecnología con fines ilegales o violentos.

Desde esta óptica, el ciberespacio como nuevo fenómeno ha cambiado radicalmente la naturaleza de las amenazas terroristas, debido a que los actores ya no se limitan a los métodos tradicionales de violencia física, sino que ahora operan de manera virtual, facilitando la expansión de su ideología y acciones a un público más amplio, y sin las restricciones geográficas que podrían haber existido antes.

Si bien, no existe un desplazamiento de la delincuencia hacia el ciberespacio -ya que este no sustituye la realidad física- sí puede afirmarse que lo complementa o la amplía, generando nuevas dinámicas para la composición de conductas punibles, pues lo actores al detectar nuevas oportunidades con menor riesgo, diversificaron su portafolio criminal; por lo que el crimen no migra sino se adapta.

Bajo este referente, el terrorismo ha mutado profundamente a lo largo del tiempo, y en la época contemporánea se ha adaptado de manera clara al ciberespacio; si bien sus raíces se encontraban ancladas a la acción directa, el terrorismo ha evolucionado a formas más sutiles que encuentran en el ciberespacio un buen lugar de expansión y aceleradas por la pandemia de COVID-19.

Como resultado de ello, existe una adaptación del terrorismo al ciberespacio que obliga a replantear su conceptualización, que se encuentra arraigada a parámetros tradicionales, para ello se creó la figura del " ciberterrorismo" propuesto en la década de 1980 por Barry Collin, el cual lo utilizó en el contexto de la transición del terrorismo del mundo físico al virtual, la intersección y fusión de estos dos mundos.

Sin embargo, la complejidad inherente de la conceptualización del terrorismo tradicional se extiende al ámbito digital, autores como Dorothy Denning (2000 citada en Poveda Criado & Torrente Barredo, 2016) lo conceptualiza como: "Ciberterrorismo es la convergencia entre terrorismo y ciberespacio. (…) Para calificar como ciberterrorismo, un ataque debe resultar en violencia contra personas o contra la propiedad, o al menos causar el daño suficiente como para generar miedo" (p. 510).

En este contexto, el ciberterrorismo es presentado como un fenómeno online que combina motivaciones ideológicas con medio propios de la ciberdelincuencia trascendiendo los límites físicos al operar en la red; de tal manera, que se diferencia de otros por su impacto simbólico y psicológico sobre la población; conforme lo establece el autor Saman Iftikhar (2024):

> El ciberterrorismo es el uso deliberado de capacidades cibernéticas, a menudo por actores no estatales, con la intención principal de causar miedo, pánico o disrupción generalizada en una población, gobierno u organización. Los actos de ciberterrorismo típicamente implican ataques motivados política, ideológica o socialmente que tienen como objetivo infraestructuras críticas,

resultan en daños significativos o representan una grave amenaza para la seguridad nacional (traducción propia, p.2).

Con ello, el ciberterrorismo congrega todos los elementos propios del terrorismo tradicional su objetivo es generar una desconfianza a gran escala a partir del miedo o el caos en aras de causar daños significativos.

Por ello lo que distingue al ciberterrorismo de otros fenómenos "como el cibercrimen o el hacktivismo, es la intención explícita de incitar el terror o desestabilizar sociedades, a menudo en busca de objetivos políticos o ideológicos, en lugar de una mera ganancia financiera o la búsqueda de objetivos sociales o éticos"(Iftikhar, 2024, p.2).

En consecuencia, los elementos constitutivos del terrorismo tradicional siguen reproduciéndose integralmente en el entorno digital, lo único que se transforma es su canal, un nuevo escenario de confrontación simbólica y operativa, pero con el mismo propósito de infundir terror y alterar los cimientos del pacto social.

Por consiguiente, se abre en la era contemporánea un medio inmaterial, intangible que puede generar daños equiparables o incluso superiores a un atentado físico; en vista de que, puede paralizar un sistema informático, sembrar miedo colectivo, manipular infraestructuras críticas, entre otros aspectos.

1. El Terrorismo Digital (TDig): una derivación contemporánea del ciberterrorismo

Ahora bien, conviene resaltar, que el ciberterrorismo al ser un fenómeno de naturaleza compleja presenta múltiples definiciones a causa de su amplio espectro de manifestaciones; por lo tanto, resulta pertinente establecer una categorización que delimite su alcance, en vista de que existen numerosas formas de su accionar que obedecen a distintos niveles de afectación de seguridad pública

La exigencia de la delimitación, obedece a que las Tecnologías de la Información y de las Comunicaciones (TIC) son un espacio amplio, que integra: la difusión instantánea de información, la interferencia de infraestructuras críticas, la manipulación de datos y la creación de miedo comunitario a través de la manera virtual

Para ello, se trae a colación la clasificación de los delitos cibernéticos como punto de referencia para establecer dicha diferenciación.

Los delitos que se desarrollan en el ciberespacio comprenden dos categorías esenciales desarrolladas por la doctrina de David Wall (2007) y Peter Grabosky (2001); pero de manera formal por el Ministerio del Reino Unido (Home Office) en su informe *Cybercrime: A Review of the Evidence* (2013), recogida por la INTERPOL en su documento *National Cybercrime Strategy Guidebook* (2021), donde retoma la siguiente clasificación:

Tabla No 1

Tipología de Delitos en el ciberespacio.

Característica	Delitos Cibernéticos Dependientes	Delitos Habilitados por la Tecnología
Dependencia Tecnológica	Esencial para la comisión del delito	Facilita la comisión del delito
Tipo de Delito	Delitos nuevos, específicos de la tecnología	Adaptaciones de delitos preexistentes
Objetivo	Sistema informático, red o datos	Víctimas, bienes o servicios
Escala	Limitada por la infraestructura cibernética	Ampliada por el alcance de la tecnología
Ejemplos	Sabotaje cibernético, hacking, malware	Fraude en línea, ciberacoso, contenido ilegal
Implicaciones	Amenaza a la seguridad, pérdidas económicas	Mayor alcance, dificultad en la investigación

Fuente: Elaboración propia en Napkin basado en INTERPOL (2021).

En el marco de los delitos cibernéticos, como se observa, existen dos dimensiones: los cibernéticos dependientes *(Cyber-dependent crimes*) los cuales comprende el uso directo de sistemas informáticos –del tipo del sabotaje cibernético– como ataques a redes o infraestructuras críticas.

Así como, los delitos habilitados por la tecnología (*Cyber- enabled crimes*), aquellos que sacan partido de la tecnología como las redes para facilitar determinadas conductas preexistentes en el ordenamiento jurídico penal.

A partir de esta dualidad, el terrorismo se abre a adoptar expresiones que le son propias de la cibercriminalidad, por lo tanto se tiene que el ciberterrorismo posee dos vertientes: El terrorismo informático y el Terrorismo Digital (TDig).

Bajo esta tipología, el componente técnico es el núcleo de la delimitación, pues, se distinguen en aquellos terroristas que emplean la tecnología como medio y aquellos que la convierten en un fin en sí mismo:

Figura No. 1

Tipos de Ciberterrorismo

Fuente: Elaboración propia en Napkin basado en INTERPOL (2021).

Atendiendo a la tipología del delito cibernético se desarrolla el ciberterrorismo, se propone esta clasificación conceptual con la finalidad de delimitar con mayor precisión el uso dañino de las TIC bajo dos dimensiones.

Por consiguiente, el terrorismo informático comprende el uso directo de tecnologías digitales, derivado de los ataques cibernéticos o de la guerra cibernética; ya que se puede pensar en el mismo como el uso de técnicas informáticas y de herramientas para atacar sistemas informáticos, redes o infraestructuras digitales, produciendo daños técnicos.

La violencia tecnológica se delimita en el uso directo de las TIC como arma de ataque, orientada a generar dañaos materiales a infraestructuras informáticas, sustituyendo la agresión de construcciones o edificios, por la agresión informática, de manera instrumental, mediante la interrupción de sistemas y flujos de información con el fin de generar colapso o desconfianza en la seguridad pública.

En cambio, el Terrorismo Digital (TDig), engloba aquellos delitos tradicionales que se ven potenciados gracias a las nuevas herramientas tecnológicas, no busca un daño técnico, busca utilizar canales digitales como el internet, plataformas virtuales "para difundir propaganda, recaudar fondos y blanquear dinero, reclutar y entrenar miembros, comunicarse y conspirar, y lanzar ataques mientras los gobiernos intentan contrarrestarlos y atraparlos utilizando medios tradicionales"(Weimann, 2006, p. 6)

El Terrorismo Digital a partir de ahora TDig, no necesita necesariamente de armas convencionales o de la ocupación física de un lugar, sino la apropiación simbólica y control estratégico de la circulación de información, la manipulación psicológica de las masas, la desestabilización social generada por campañas de desinformación, e incluso la propaganda radical son suficientes para ocasionar caos, inseguridad o presión política.

Para el TDig, el control de la información y la influencia de las masas es vital para su desarrollo, convirtiéndose en armas más letales que los propios explosivos, bien lo decía Manuel Castells (2009), en la sociedad-de la información "el poder reside en la capacidad de construir significados compartidos en los flujos de comunicación"(p.10) y justamente ahí radica su fuerza.

La batalla no se efectúa con armas ordinarias, ni tampoco en espacios geográficos con límites concretos, sino que ahora tiene lugar en el ciberespacio, donde la gran red (internet) y las plataformas sociales representan el ámbito del escenario del conflicto.

El clima del internet es tan fructífero que según Thomas Timothy (2003), es perfecto para que un grupo radical explique sus acciones o contrarreste la condena tanto interna como internacional,

especialmente al utilizar servidores específicos. Internet puede atacar tanto a indecisos como a creyentes con diferentes mensajes, orientados a su público objetivo.

De igual manera, autores como Sara Zeiger y Joseph Gyte (2020) expresan que los miembros de los grupos terroristas contemporáneos han crecido con la implementación de la tecnología y con ello con el acceso a internet y redes sociales; circunstancia que explica porque en la actualidad estas plataformas desempeñan un papel fundamental en su accionar delictivo.

En virtud de ello, la finalidad del TDig se dirige a afectar a la población civil en general, a la opinión pública e incluso la estabilidad política por medio de plataformas que expenden la influencia de los grupos terroristas más allá de su capacidad operativa real, por las estrategias adoptadas en ella, sembrando terror, odio o polarización en la sociedad mediante el uso estratégico de los recursos tecnológicos. .

Con todo el TDig se define como una derivación del ciberterrorismo por cuanto su forma de violencia tecnológica se encuentra en el plano comunicacional de las TIC: usando redes, plataformas y medios digitales; en aras de difundir miedo, odio o desinformación, con el fin de afectar a la población civil o parte de ella, manipular la opinión pública y desestabilizar la estabilidad social o política ; ya que socava de manera silenciosa los propios pilares del orden democrático la confianza, y la seguridad digital derivada de la seguridad pública.

En efecto, el TDig se configura como una amenaza directa al bien jurídico de la seguridad digital, concebida como una manifestaciones la seguridad pública, en tanto busca salvaguardar a la población frente a actos dañinos para el pacto social , mediante el uso indebido de las TIC bajo el marco comunicacional digital (no físico, no técnico).

Si bien, las redes sociales, foros, blogs, webs han tomado iniciativa en aras de generar reglamentos que le faciliten la no tolerancia frente a organizaciones terroristas, siguen siendo espacios

de escaso control jurídico y social; e incluso al comenzar a delimitar este campo, las células terroristas encuentran en la Deep Web y en el segmento de la Dark Web un medio idóneo para continuar con sus actividades ilegales de manera clandestina y sin ningún tipo de rastro.

No obstante, no son los únicos escenarios, el uso de criptomonedas para su financiamiento, la utilización de inteligencia artificial para hacer más efectivo su actuar, e incluso el metaverso se convierte en amenazas potenciales.

Personajes como Samar Violeta Francisco Agra (2022) han ido expresando su verdadera preocupación , en aquellos espacios que poseen una inmersión digital como el metaverso, porque si bien, puede realizarse estrategias intrínsecas de su actuar, poco se habla de la repercusión psicológica de un ataque en dicho espacio.

Con esto en mente , los terroristas intentan hacerse con la atención, con el discurso, e incluso con las emociones de la opinión pública, y en tal sentido la información y la tecnología se convierten en medios de coerción ideológica.

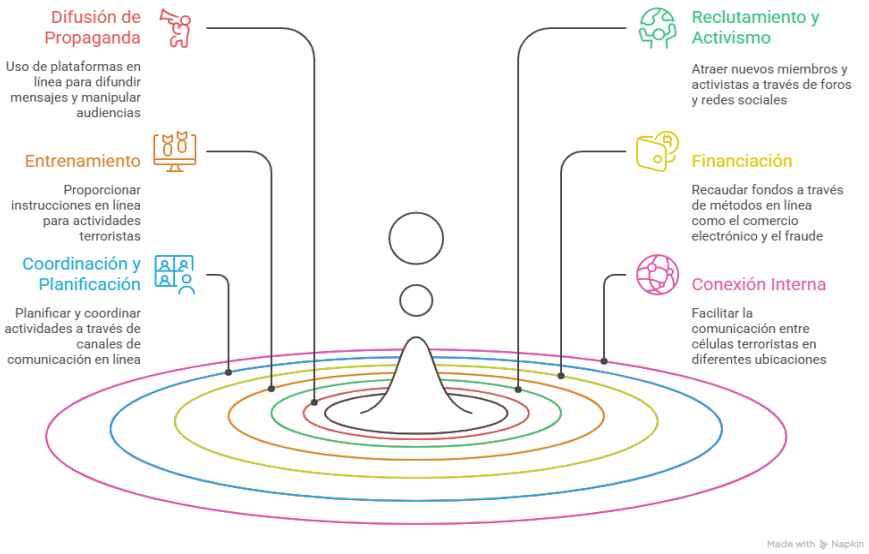
El paso a lo cibernético convierte el acto terrorista en un medio para la influencia de un todo, el de una estrategia de efectos globales, una estrategia de influencia capaz de extenderse en el tiempo y en el espacio.

La instrumentalización del entorno digital para facilitar sus prácticas ilícitas, incrementa su impacto. De ahí, que el TDig presente un conjunto de estrategias que, desplegadas en el ámbito virtual, van destinadas a provocar miedo, segmentar a la sociedad, desgastar a las estructuras estatales, así como a imponer y dar cauce a unas ideologías extremistas, y todo ello sin necesidad de violencia física directa.

El desarrollo de estas estrategias a través de canalizaciones digitales puede caracterizarse por un carácter flexible, anónimo, y apto para generar efectos simbólicos y políticos de gran proyección, su materialización en el ciberespacio se encuentra desarrollado por un actuar común:

Figura No. 2

Estrategias que desarrolla el Terrorismo Digital (TDig).



Fuente: Elaboración propia en Napkin basado en Poveda Criado, M. & Torrente Barredo, B. (2016).

Las estrategias comentadas, convergen en ser un campo extenso que ha sido ampliamente abordado por distintos doctrinantes en especial la Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC) por ser una amenaza de gran impacto a nivel trasnacional, ya que , su básica asimetría, anonimato y bajo coste lo convierten en especial peligro para los Estados modernos.

Hecha esta salvedad, la violencia tecnológica del TDig, se manifiesta en el plano comunicacional o simbólico de las TIC, es decir a través de la gran red, que contempla: redes sociales,

plataformas de comunicación, videos, foros, entre otros; aprovechando la difusión instantánea de la información y la vulnerabilidad emocional de las audiencias.

Para finalizar, si bien, sí existe un reconocimiento pleno de la amenaza que constituyen las tecnologías de la información y la comunicación (TIC) en los actos terroristas, no se encuentra como prioridad dentro de la agenda, por cuanto todo se deja al margen de la cooperación internacional y normatividad interna.

La mayoría de convenciones, como la Convención Interamericana contra el Terrorismo (2002) de la OEA, o las resoluciones del Consejo de Seguridad de la ONU, continúan el desarrollo de un terrorismo tradicional, en conjunto con otros instrumentos internacionales referenciados en todo el apartado. Poco se habla de la prioridad de guiar a nivel global las actuaciones ilícitas que excedan el pacto social.

El propósito de derecho penal internacional se ve obstaculizado conforme avanzan las estrategias empleadas por los grupos terroristas, sumado a la incapacidad técnica e institucional de la comunidad internacional, para hacer frente de manera ostensible a este dilema.

La evolución del terrorismo al ciberespacio evidencia una profunda transformación las nuevas dinámicas delictivas contemporáneos, donde la violencia digital, es el medio instrumental por excelencia; bajo este contexto se presenta el TDig como nueva amenaza desafiando los límites del poder punitivo y la capacidad del derecho penal internacional para salvaguardar la seguridad digital como bien jurídico a proteger.

Esta circunstancia permite ineludiblemente reflexionar acerca de los modelos de respuesta penal ante situaciones extremas que sobrepasan las fronteras físicas y jurídicas tradicionales.

2. Terrorismo Digital (TDig), Enemigo Y Sociedad Del Riesgo

En ese marco, la figura del terrorismo tradicional deriva de un campo excepcional de la esfera del delito; pues su naturaleza implica una violencia singularmente diseñada para subvertir el orden, influir en la política y sembrar el terror en sociedad; debilitando así el pacto social.

El fenómeno se sitúa más allá del derecho penal clásico; ya que busca destruir el contrato social vigente al no servir a sus intereses. De esta manera, el terrorismo actúa como acto comunicativo al utilizar la violencia directa como medio de transmisión simbólica orientada a infundir terror en la población -apartada de toda benevolencia del DIH- con el fin de aniquilar el orden político vigente.

Su esencia, no obedece a un delito ordinario sino a una amenaza estructural "sui generis" cuyo objetivo está en el declive del tejido del orden constitucional que erige un sistema, por lo que permite justificar medidas extraordinarias por parte del Estado en aras de proteger a la sociedad ante un posible riesgo a gran escala.

Al existir un abandono al proyecto en comunidad de manera voluntaria -por parte de quienes hacen parte de organizaciones criminales que se dirigen a materializar este fenómeno- cualquiera de sus integrantes ya ostentan un rótulo de "enemigo interno".

Como sostiene Jakobs (2003), este tipo de sujetos no prestan la garantía cognitiva mínima necesaria para ser tratados como personas, lo que significa que han abandonado el derecho penal ciudadano y han de situarse dentro del marco del Derecho Penal del Enemigo.

El jurista Isidoro Aramburo (2015) confirma esta aseveración, al considerar que el esquema propio de la Teoría del Derecho Penal del Enemigo, desde ahora TDPE está supeditado a un tipo criminal específico que actúa de forma persistente y representa un peligro constante: el terrorismo que aunque no el único, es el máximo exponente.

Continuando con este razonamiento, para Pablo Elías González Monguí (2019) los individuos peligrosos o quienes materializan la figura del enemigo:

> (...) serían aquellos que pertenecen a la criminalidad económica, al terrorismo (Bernal Castro, 2018), a la criminalidad organizada que se expresa como delincuencia común, al narcotráfico (González Monguí y Villarreal Correcha, 2015), a la delincuencia política y al concierto para delinquir. También podrían caber otros que actúan individualmente como los delincuentes sexuales y los autores de "otras infracciones penales peligrosas", que el autor deja como abiertas, posiblemente para que dadas las circunstancias se califiquen como potencialmente realizables por éstos (p. 1074).

Si se sigue con este argumento, el terrorismo daría pie a la aplicación de un derecho penal de guerra o de supervivencia, cuyo objetivo ya no sería el de la reeducación o la reinserción, sino tan solo el evitar el peligro, la neutralización preventiva del mismo.

Por lo tanto, puede afirmarse que el terrorismo tradicional es la manifestación practica (la especie) que describe y sustenta la TDPE ofrecida por Jakobs (el género). Este fenómeno, es precisamente a lo que el profesor alemán se refiere cuando advierte que los sistemas garantistas penales contemporáneos ya aplican prácticas propias de esta teoría; podría decirse "por debajo de la mesa".

Es menester destacar, que el autor no pretende promover este derecho, por el contrario considera deseable su inexistencia; sin embargo, su objetivo se encauza en la descripción de un comportamiento real del sistema, pues aunque los Estados se jactan de aplicar un derecho penal del ciudadano, en la práctica coexisten con un derecho penal encubierto dirigido a la neutralización de quienes perciben como peligrosos.

En síntesis, el terrorismo representa el ejemplo paradigmático que explica la razón de ser de la TDPE : un derecho orientado al control del peligro más que a la juridicidad, que transforma al

ciudadano en objeto de neutralización -no persona- cuando decide romper definitivamente su vínculo con el Derecho y la seguridad pública.

En verbigracia, a partir de los atentados del 11 de septiembre de 2001, el terrorismo, que antes se consolidaba en ámbitos locales, adquirió una dimensión internacional, lo que produjo una respuesta por parte de la comunidad internacional concentrada en la doctrina norteamericana y avalado por la Naciones Unidas.

En aras de contrarrestar estos actos, se creó un ordenamiento jurídico anticipado, encarnado en el ámbito penal orientado a la gestión del peligro, donde el Estado asume una función eminentemente preventiva. La legitimidad del actuar del Estado se mide por su capacidad de neutralizar amenazas antes de que se materialicen, una expresión clara de la TDPE.

En esa misma línea preventiva frente a riesgos a escala global, y una vez comprendido el impacto global del terrorismo, resulta esencial abordar el papel desempeñado por la ONU, a través del Consejo de Seguridad como organismo encargado del mantenimiento de la paz y la seguridad internacional, el cual ha impartido resoluciones vinculantes para los Estados miembros, frente a la expansión del terrorismo.

Las resoluciones, están orientadas a prevenir y desmantelar el "terrorista" en el momento previo a la acción, pudiendo llegar a imponer sanciones que debilitan a los grupos y anticipan la punibilidad por temor a los costos que suponen los riesgos tecnológicos.

Esta mutación del modelo punitivo no puede comprenderse sin recurrir a la teoría de la sociedad del riesgo de Ulrich Beck (1986), quien advierte que la sociedades actuales viven de manera consciente y continúa de la existencia del peligro; cuyo origen no son los factores externos como la naturaleza, sino las propias acciones internas de la especie en aras de consolidar su progreso.

Esta situación es denominada como "sociedad de riesgo" , donde el riesgo deja de ser la excepción a la regla y se convierte en una condición determinante de la vida en sociedad.

La evolución del ser humano en sociedad se encuentra ligada al avance técnico y científico, el cual es amplificado por el fenómeno de la globalización que deriva en una interdependencia entre los Estados, en conjunto con avances de las nuevas tecnologías.

De acuerdo con la doctrinante Luz Mary Rincón Romero (2016):

> La sociedad del riesgo ayuda a la consolidación y nacimiento del derecho penal del enemigo, en el sentido que esta produce la flexibilización de las normas de imputación penal, dejando de lado aspectos elementales de la misma, adecuando la técnica legislativa de crear una norma penal que castigue actos preparatorios (p. 307).

Bajo este enfoque, los subsistemas que permiten la materialización de la convivencia social, se encuentran en un estado de vulnerabilidad permanente; ante el continuo surgimiento de avances que se constituyen como amenazas inminentes y difusas para el entorno.

Según la jurista Natalia Andrea Bravo Peña (2007) "La sociedad del riesgo es consecuencia directa del temor al exterminio global. Tememos aquello que nos puede afectar a todos, no aquello que se puede sectorizar. Hoy los temores son globales, el riesgo ya no es para algunos sino que para todos" (p.86).

De allí que, el eje de la vida social, lejos de enfocarse en la búsqueda de un bienestar común, se encuentra enfocado en la administración del riesgo, pues lejos de sucumbir ante este fenómeno, se busca enfrentarlo desarrollando mecanismos para preservar el orden colectivo, cuyo protagonista es el derecho penal.

Tal como señala Hassemer (1991), dicha demanda de seguridad deriva en un proceso de expansión del Derecho Penal, puesto que sirve como una forma de dar seguridad a la comunidad frente a los miedos que identifican a la población.

Así, el terrorismo —como expresión extrema de riesgo político y existencial— se integra a ese imaginario de amenazas constantes y difusas, cuyo combate se hace a partir de estrategias de control de riesgo ante la estabilidad colectiva que justifica su tratamiento diferenciado.

Esta perspectiva está determinada por varios fundamentos teóricos de la TDPE, entre ellos la prevención absoluta ante amenazas futuras y anticipación punitiva.

Por consiguiente, el terrorismo se convierte en un estímulo que enlaza al derecho penal con la teoría de la sociedad del riesgo: un derecho de prevención de riesgos futuros. Un modelo que identifica y neutraliza el peligro y lo anticipa antes de que se produzca. Bajo esta lógica, el Estado gestiona la incertidumbre no solo con la sanción, sino que vigila, controla, previene.

En la situación actual, este mismo razonamiento de anticipación y gestión del riesgo se proyecta al ciberespacio, un entorno que amplía las fronteras del conflicto, multiplicando las fuentes de amenaza en el ámbito virtual. En el ciberespacio, ciudadano y enemigo se diluyen; ya que el actuar se representa por el anonimato, la transnacionalidad, y la descentralización provocando un impacto considerable.

El ciberespacio en su ámbito virtual, (como se observó en el marco teórico del primer capítulo) ha dejado se ser un mero entorno tecnológico aislado de la sociedad; por el contrario, en la actualidad convergen dinámicas sociales, económicas, políticas y culturales de alcance global.

No obstante, pese a su potencial como herramienta de progreso, ha contribuido a ser un territorio de vulnerabilidad que escapa de la regulación de los Estados, por su novedad.

Manuel Castells (2009) en su obra "*La era de la información",* señala que el poder no se ejerce sobre territorios físicos, sino en flujos de información del plano virtual. Este desplazamiento implica a su vez un traslado del conflicto a este nuevo ámbito; representando una nueva forma de riesgo y vulnerabilidad, que trascienden las fronteras físicas del Estado y desafían su capacidad de control .

Por consiguiente, la naturaleza del ciberespacio genera nuevos escenarios de riesgo al ser una extensión de la realidad, pero sin las barreras jurídicas que estructuran el mundo material, pues a pesar de ser una infraestructura esencial existe una ausencia de regulación efectiva, favoreciendo el surgimiento de nuevas formas de criminalidad o la reproducción fidedigna de esta en el entorno digital.

Ahora, con la pandemia COVID 19, coadyuvo a que existirá un incremento sin precedentes de la dependencia de la TICs, debido a que " supuso un nuevo acelerón en la digitalización de la sociedad, traducido en el crecimiento del uso de internet en general y de las redes sociales en particular"(Cardeño, 2021, p.102).

Lo anterior, fue gracias a que para mitigar el impacto socioeconómico de la crisis sanitaria se desarrolló una virtualización forzada que magnificó la exposición de las personas a este riesgo, produciendo nuevas vulnerabilidades y oportunidades para la comisión de delitos cibernéticos, exacerbando la necesidad de respuestas penales adaptadas a este nuevo entorno digital.

La expansión del ciberdelito comenzó a tensar el delito común y evolucionó en prácticas más agresivas desestabilizadoras del pacto social, logrando un nuevo escenario operativo para grupos terroristas que potencian sus estrategias tradicionales desde el entorno virtual reproduciendo la lógica del miedo con mayor eficacia, rapidez y cobertura.

Dentro del margen aplicable, el TDig, representa una mutación ontológica del riesgo, en vista de que en el escenario ha cambiado; ya que, su objetivo no es el daño físico inmediato, sino el colapso del vínculo social del propio tejido colectivo desde la guerra psicológica y cultural a partir de la

instrumentalización de las plataformas, donde la agresión no se mide en bajas materiales, sino en pérdida de confianza comunicativa.

El terrorista digital no reconoce el orden jurídico, no se somete a las reglas del discurso democrático y opera desde la negación de la expectativa normativa, no se está ante un infractor común, sino un actor que utiliza la libertad comunicativa y tecnológica —los propios medios contemporáneos— para destruir sus cimientos, su manifestación natural: representa la antítesis del ciudadano normativo y encarna la ruptura entre el Derecho y la conducta socialmente esperada.

En este orden de ideas, se podría afirmar sin ningún tipo de dudas que el TDig es, por así decirlo, una representación del TDPE; no porque la normatividad lo establezca sino porque su práctica encarna la lógica de profesor Jakobs, que es aquella por la que el sujeto se autoexcluye del pacto normativo, renuncia a ser un ciudadano y se convierte en un riesgo permanente.

El TDig además de ser una amenaza revela los propios límites del derecho penal en la actualidad, por la que el Estado pasa a preguntarse su capacidad de respuesta ante quienes no reconocen su legitimidad dentro del ciberespacio.

Partiendo de este marco, donde el TDig es una expansión del radio de acción del terrorismo en plataformas virtuales, siéndole inherente la encarnación de la figura del enemigo al ser aquel que niega el pacto normativo y busca desestructurar la convivencia mediante el uso del ciberespacio. Se hace necesario examinar cómo el Estado colombiano ha intentado afrontar este fenómeno dentro de su propio ordenamiento jurídico.

Entre 2020 a 2025, en lo referente al fenómeno del TDig la respuesta del Estado Colombiano; a pesar de constituir una amenaza latente acelerada por la pandemia COVID-19, aún carece de una regulación específica dentro del marco del derecho penal que sigue anclado a la realidad material, y no a las nuevas dinámicas del ciberespacio.

En efecto, ninguno de los tipos penales previstos tanto en Título VII BIS y Titulo XII (art. 343, 344, 345, 348) del Código Penal es capaz de dar cuenta de la complejidad del fenómeno del TDig, ni permiten abordar de manera integrada sus formas de manifestación, tales como la radicalización en línea, el adoctrinamiento, la propaganda extremista o la coordinación de actos de violencia.

El tratamiento jurídico del terrorismo en Colombia se mantiene dentro de un enfoque clásico, reducido a la acción violenta, el medio empleado y la capacidad de generar un estado de zozobra o terror de manera colectiva en su normatividad; de ahí, se entiende este fenómeno, en su versión tradicional, como un peligro para el Estado y la sociedad.

En esa línea, la Corte Constitucional, a su vez, y la Corte Suprema de Justicia también dieron paso a una lectura del terrorismo que es punitiva y preventiva, sujeta a la búsqueda del respeto por el orden público al igual que de la protección de la población civil y del cumplimiento de las obligaciones internacionales del Estado que tiene que ver con la lucha frente a este fenómeno.

No obstante, la concentración de estas categorías de reflexión en el ámbito digital, entre los años 2020 a 2025, es que el TDig, hasta el día de hoy, a pesar de que se puede considerar como una amenaza inminente dada la aceleración del panorama en post pandemia, todavía sigue adoleciendo de vías específicas y de una regulación sistemática dentro del derecho penal colombiano, que más bien permanece fijado a una realidad material que a las dinámicas propias del ciberespacio.

Considerando que no existe un tipo penal que desarrolle plenamente sus vertientes en Colombia el análisis no se detiene en la parte sancionadora, resulta ineludible transitar hacia el terreno donde se ha estructurado la respuesta estatal como corresponde, lo que equivale a la política pública de seguridad digital.

Respecto a las políticas, quien desarrolla lo atinente al tema es el CONPES (Consejo Nacional de Política Económica y Social), los cuales elaboran instrumentos de planeación estratégica de políticas

del Estado necesarias para su desarrollo; pero en particular, políticas dirigidas a la seguridad, la defensa, la tecnología, la educación, entre otras. Configurando una respuesta preventiva y estructural frente a riesgos emergentes.

Es preciso determinar, que los documentos CONPES no regulan directamente conductas como el TDig, pero sí integran una zona donde el Estado reconoce y gestiona amenazas derivadas del ciberespacio que afectan la seguridad nacional, cumpliendo una función tanto de prevención como de mitigación a partir de definir líneas de acción institucional, identificar variables estructurales, y fortalecer capacidades de defensa.

Ahora bien, Colombia ha venido adoptando documentos CONPES de ciberseguridad desde etapas tempranas; en verbigracia, el CONPES 3701 de 2011 (Política de Ciberseguridad y Ciberdefensa) y el CONPES 3854 de 2016 (Política Nacional de Seguridad Digital), los cuales fueron los primeros pilares que comenzaron a edificar la política nacional de ciberseguridad y seguridad digital, como consecuencia de las amenazas informáticas y nuevas vulnerabilidades tecnológicas.

En el periodo 2020 a 2025, y específicamente frente a la atipicidad del TDig, es pertinente dirigirse a los CONPES 3995 de 2020 (Política Nacional de Seguridad Digital) y el CONPES 4144 de 2025 (Estrategia Nacional de Inteligencia Artificial), por tratarse del escenario institucional más cercano donde pueden expresarse lógicas de control y prevención compatibles con la racionalidad de lo que se concibe como TDPE.

Cabe destacar, que ninguna de las dos políticas referenciadas crea conductas punibles o incluso fija penas, por el contrario, su desarrollo se centra en la organización de una forma de gobierno del ciberespacio que privilegia la prevención, el control y la administración de riesgos antes que la retribución.

En primer lugar, el CONPES 3995 de 2020 (Política Nacional de Seguridad Digital) parte de una noción de "seguridad digital" asociada a normalidad y tranquilidad del sistema, y desde ahí construye una lógica funcionalista, en donde, lo importante es sostener la estabilidad del entorno digital nacional. Para ello, introduce mecanismos de educación, vigilancia, cooperación institucional e internacional y neutralización anticipada de amenazas.

Aunque, no habla explícitamente de "enemigos", sí establece una diferencia simbólica entre actores confiables —los "ciudadanos digitales" que se alinean con la política de confianza— y actores que aparecen como amenazas o riesgos para esa normalidad. Esa frontera no es penal, pero sí política: separa a quienes garantizan la continuidad del sistema de quienes la comprometen.

En ese sentido, el CONPES no castiga a un enemigo, pero sí organiza una vigilancia preventiva basada más en lo que los sujetos podrían llegar a hacer (según su comportamiento digital) que en un daño ya consumado.

En cuanto al TDig, el concepto de amenaza, constituye un primer vestigio al establecer a aquellos actores que realicen acciones capaces de alterar la integridad de la información, incorporando el ámbito simbólico e informativo como espacio vulnerable del ciberespacio.

Así, cuando esta alteración se produce de manera intencional; con el fin de causar daño generando una desestabilización de la sociedad, se configura un escenario equiparable al TDig, aunque continue sin piso jurídico.

En segundo lugar, el CONPES 4144 de 2025 (Estrategia Nacional de Inteligencia Artificial) sigue un paso más en esa lógica al hacer de la inteligencia artificial el eje central de la estrategia estatal. Su promesa es muy digna, utilizar la IA para derechos, innovación y desarrollo; sin embargo, su organización permite ver un fondo igualmente anticipatorio: la prevención del daño se reduce a modelos predictivos, alarmas tempranas y vigilancia algorítmica.

A su vez, institucionaliza una ética de la IA de carácter normativo que, aunque suene como una garantía, cumple también una función clasificatoria: actores "éticos" que son parte del sistema y actores "no éticos" que quedan bajo sospecha de ser riesgosos. No los convierte en enemigos penales, pero sí en sujetos vigilables.

Bajo el paraguas de la confianza digital y la seguridad el Estado desplaza la idea de justicia por la idea de administración del riesgo, convirtiendo a la IA en el nuevo instrumento de regulación del orden social.

De forma que el ciudadano ya no es protegido como sujeto de derechos sino observado como una mera amenaza potencial, dentro de un paradigma en el que la prevención reemplaza al derecho y donde la eficiencia técnica se impone.

Así las cosas, ambos documentos se encuentran en una tendencia hacia un funcionalismo sistemático lo que refleja que no existe, en primer lugar, lógicas punitivas por cuanto su órbita se cimienta en el derecho administrativo.

Es decir, no existe un enemigo en el estricto sentido de la TDPE, sino que se diluye en un riesgo administrable por el Estado, en pro de garantizar una seguridad digital para los distintos actores que interactúan en el ciberespacio.

En este caso no se plantea una expulsión del ordenamiento jurídico ordinario del actor, sino una vigilancia constante del Estado con respecto al uso de las nuevas tecnologías para evitar futuros daños.

En estas políticas de manera implícita se busca administrar y garantizar un comportamiento adecuado, por lo que el enemigo debe ser adoptado desde el riesgo, en otras palabras, ya no es una -no persona- es un sujeto de gestión, vigilado, prevenido y administrado por el Estado.

La sanción queda como superada por la administración y la administración se presenta como cuidado. Como bien explica Shoshana Zuboff (2019), esta combinación Estado y tecnología hace que la prevención sea un nuevo modo de gobierno; la seguridad se autojustifica y vigila en nombre de la protección.

Michel Foucault (2007) desarrolló el argumento de que el poder actual ha dejado de necesitar la exclusión como medio para el dominio y es suficiente con la regulación de la vida.

La biopolítica deviene ciberpolítica y el enemigo se transforma en el dato, en la anomalía dentro de un sistema informacional. El Estado no sólo deja de castigar la desviación, sino que sigue la variación.

Según Tuset (2024) "La vigilancia en la era digital se asemeja cada vez más al panóptico foucaultiano, donde la posibilidad de una observación constante influye en el comportamiento, incluso si la observación no es continua."

De este modo, el Estado colombiano no adopta la TDPE, pero incorpora de manera reducida sus efectos simbólicos y funcionales en la gestión de la seguridad digital.

En definitiva, el TDig en Colombia ha sido considerado, en su mayor parte, como un riesgo administrable; donde el Estado intenta controlar y contener el fenómeno por medio de la prevención, las formas de vigilancia, la cooperación institucional y también mediante el uso de la técnica, sin llegar a la autonomización penal.

Sin embargo, tal movimiento hacia la prevención no suprime el problema de fondo, sino que lo desplaza a otro nivel: pues el TDig, es considerado en primer lugar como un riesgo administrable pero su potencialidad de causar daño colectivo puede requerir una respuesta jurídica más fuerte; lo

malicioso es que la cuestión es cómo sostener tal tránsito sin que la anticipación preventiva se convierta, por mera inercia, en forma de Derecho Penal del Enemigo.

Es por ello que la explicación debe ahora pasar por el Estado Social de Derecho (ESD), es decir, el marco normativo de la Constitución de 1991 que fija los límites y condiciones de legitimidad para cualquier intervención que el Estado realice frente a amenazas extremas en el ciberespacio.

3. Estado Social De Derecho (ESD): Desafíos ante el Terrorismo Digital (TDig)

El primer artículo de la Constitución Política de Colombia (1991) consagra de manera taxativa la forma de organización del Estado, amparado bajo un Estado Social de Derecho (ESD) que reconoce la dignidad humana, el trabajo, la solidaridad y la prevalencia del interés general como pilares esenciales de su orden político y jurídico (Colombia. Asamblea Nacional Constituyente, 1991, art. 1).

Bajo esta fórmula, se consolida la identidad jurídica, filosófica y política del Estado colombiano, lo cual, significó un cambio de paradigma entre la relación Estado/Particular al consolidar desde una visión antropocentrista el Estado al servicio del ser humano.

La supremacía constitucional, ha derivado en la constitucionalización del derecho, en especial, del derecho penal, en vista de que el Ius Puniendi del Estado, queda supeditado a los parámetros (valores, principios, derechos) constitucionales. La Corte Constitucional en sentencia C-038 de 1995 ha dispuesto:

> Ha habido una constitucionalización del derecho penal porque tanto en materia sustantiva como procedimental, la Carta incorpora preceptos y enuncia valores y postulados - particularmente en el campo de los derechos fundamentales - que inciden de manera significativa en el derecho penal y, a la vez, orientan y determinan su alcance (M.P. Alejandro Martínez Caballero).

Bajo este referente, el derecho penal se convierte en un instrumento de protección de bienes jurídicos, guiado por los principios de la carta constitucional, en especial por la dignidad humana, desplazando la relación de Estado/Particular, donde el primero sirve al último dentro del marco punitivo.

Por eso, la norma penal no se legitima solo por su validez formal, sino por su coherencia axiológica con el Estado Social de Derecho desde ahora ESD, lo que desplaza la relación Estado-persona hacia un modelo antropocéntrico donde el derecho penal existe para proteger bienes jurídicos y garantías, no para ejercer control moral o exclusión.

De tal giro, se desprende que la potestad punitiva es un poder racionalizado y limitado: su fin no es la retribución como tal, sino la protección del ser humano frente a abusos estatales.

De manera que el derecho penal sólo funciona de acuerdo con el principio de mínima intervención o ultima ratio, es decir, no se encuentra en funcionamiento hasta tanto no hayan dado sus frutos otros mecanismos de control y en situaciones de conductas que lesionan de manera grave bienes de la vida social o que implican un riesgo directo para la comunidad (C-365/12 M.P.: Jorge Ignacio Pretelt Chaljub, C-233/19 M.P.: Luis Guillermo Guerrero Pérez).

La lógica jurisprudencial de carácter constitucional refleja el garantismo penal propio de Ferrajoli, donde el derecho penal ya no es un instrumento de control social, sino un instrumento encaminado a proteger garantías fundamentale, el castigo solo tiene sentido si es necesario para garantizar derechos. La excepción y el miedo no expanden arbitrariamente la potestad punitiva.

Finalmente, ese garantismo se caracteriza por los límites materiales al ius puniendi: legalidad (no puede haber ni delito ni pena sin ley anterior, clara y escrita), culpabilidad (no hay pena sin responsabilidad probada; derecho penal de acto y no de autor), proporcionalidad (prohibición del exceso punitivo: la pena debe ser imprescindible y equilibrada con el daño y la culpabilidad) y la

humanidad de las penas (la sanción no puede degradar ni anular la condición humana, tiene que respetar la dignidad y tiene que ir en la dirección de la reintegración).

Tanto la jurisprudencia constitucional como la doctrina afirman que esos límites -explícitos o implícitos- hacen del derecho penal un sistema de límites políticos y morales frente al Estado-tales principios no van a quedar reducidos a simples normas de técnica jurídica, sino que van a describir auténticas garantías políticas y morales protectoras frente al Estado.

Las anteriores consideraciones, permiten afirmar que el único derecho penal que es permitido por el ESD, desde el funcionalismo, es el funcionalismo teleológico de Claus Roxin.

Bajo esta perspectiva, es previsible que la visión garantista que contempla el ESD derive en un conflicto claro frente a los fundamentos teóricos del Derecho Penal del Enemigo de Gunter Jakobs.

Para el ESD la creación de este sistema ya comporta una frontal contradicción con los principios estructurales y axiológicos que sostienen el orden jurídico, pues su problema no es solo técnico, sino de fondo: al partir de la división entre "ciudadanos" y "enemigos", convierte a ciertos sujetos en "no personas", lo que implica negarles la dignidad que el ESD reconoce incluso a quien delinque.

Esa misma dicotomía rompe la igualdad ante la ley, porque introduce un derecho penal dual donde unos conservan garantías y otros quedan sometidos a reglas excepcionales según su supuesta peligrosidad.

Además, la lógica funcionalista que lo sostiene desplaza el sentido garantista del derecho penal: ya no se protege a la persona y sus derechos, sino que se prioriza la preservación del sistema y la neutralización anticipada del riesgo.

De ahí se desprende su efecto más grave: la afectación de garantías procesales como la presunción de inocencia, la defensa y la proporcionalidad, pues el castigo deja de basarse en hechos probados para apoyarse en perfiles, sospechas o identidades consideradas amenazantes

En definitiva, la TDPE constituye una profunda y grave amenaza para los límites del ius puniendi en un ESD, pues su naturaleza está dada en ser mecanismo de exclusión más que en proteger bienes jurídicos.

La racionalidad preventiva, de las políticas comparadas, debe dejar de estar anclada a la mera gestión técnica del riesgo, debe supeditarse en el marco del Estado Social de Derecho (ESD) requiere una mutación en el sentido de una seguridad digital garantista, en la que la protección de amenazas digitales no se logre en detrimento de los derechos fundamentales, sino más bien a la luz de ellos.

Lo que requiere entre otras cosas, asumir que la seguridad, en el plano digital, no es una mera finalidad técnica sino una categoría jurídica que necesita ser interpretada atendiendo los principios constitucionales de legalidad, proporcionalidad y dignidad humana, parámetros que ya han sido abordados por pronunciamientos internacionales como los tribunales europeos.

Una política pública efectiva verdaderamente democrática en pregunta de lo digital no puede fundarse en la opacidad de los algoritmos, ni en la lógica del control total, sino en la transparencia algorítmica, el control judicial efectivo y la responsabilidad institucional en la cuestión del tratamiento de los datos.

Por último, al comparar ambos documentos se observa que hay una tendencia en descenso sobre lógicas punitivas o de control, y un avance progresivo en la inclusión de un enfoque garantista. El último CONPES se encuentra en un punto de madurez institucional, ya que ha asumido el desarrollado de los derechos fundamentales de la ciudadanía como eje en el marco de la inteligencia artificial.

En este sentido, el gran reto consiste en saber traducir el reconocimiento formal de los derechos en otros mecanismos reales de control, supervisión y responsabilidad estatal de la esfera pública que de alguna manera contribuyan a construir una verdadera seguridad digital con rostro humano.

Esto de igual manera, debe darse en el ejercicio del ius puniendi, este debe está subordinado de manera categórica a los principios del ESD, entre ellos la dignidad humana, los cuales, no son simbólicos u opcionales, deben prevalecer de manera integral en la práctica penal sin excepción, pues son mandatos de obligatorio cumplimiento.

El reto del Estado colombiano, se encuentra frente a conductas particularmente graves que vulneran de manera latente el pacto social, pues debe buscar conciliar la seguridad pública con las garantías fundamentales, cuyo criterio orientador se encuentra en la dignidad, adoptando un derecho penal como mecanismo de control social, pero más como instrumento de garantías y no de venganza.

En este punto, como debería entonces el ESD enfrentar amenazas digitales que trascienden el riesgo administrativo y se encuadran como conductas punibles que repercuten en la vida social de las personas; en otras palabras, ¿Cómo responder penalmente a riesgos digitales que todavía no son delitos, sin caer en la lógica de la exclusión de la TDPE que pretendía superar?

Es claro que estas conductas punibles no van a desaparecer por cuanto comprenden una afectación directa al sistema social, no obstante, el Estado no puede reaccionar ante ellos de manera desmedida pues estaría al mismo tiempo desconociendo su base fundacional. Esta situación comienza a visibilizar los limites frente garantismo penal cuando esta frente a transformaciones del mundo contemporáneo.

En verbigracia, la política pública no basta para neutralizar la amenaza latente que es el TDig, el ESD no puede permanecer inerte ante la apropiación simbólica y control estratégico de las

circulación de información, la manipulación psicológica de las masas, la desestabilización social generada por campañas de desinformación, e incluso la propaganda que actores pueden desplegar en el ciberespacio, pues desestabilizan el orden social; pero tampoco puede responder desde la exclusión y el desarrollo de la categoría de -no persona-.

Es en esta línea donde empieza la propuesta de Silva Sánchez (2001) de un garantismo penal dinámico o activo. No se propone arrinconar el garantismo ferrajoliano, sino superar su inmovilidad ante los nuevos riesgos sociales que reclaman de la intervención penal razonable.

Así, el TDig se nos propone como un claro ejemplo de sociedad del riesgo: una forma de violencia simbólica y psicológica que busca provocar una colapso del vínculo social, y que afecta a un bien jurídico contemporáneo: la seguridad digital como manifestación de la seguridad pública, sin que tenga que provocar necesariamente una destrucción física inmediata.

La expansión del derecho penal puede, no obstante, ser legítima cuando se justifica en razones razonables (necesidad de proteger bienes jurídicos actuales, riesgos tecnológicos, crecientes afectaciones colectivas); y en cambio puede ser considerada ilegítima cuando se desvirtué en populismo punitivo, delitos simbólicos redundantes o cuando en ella se limite la garantía individual de forma arbitraria.

Aplicado al ámbito colombiano, convertirse en un delito autónomo el TDig, causaría una grave vulneración del principio de legalidad por dos razones terminantes:

En primer lugar, su estructura abierta imposibilitaría un tipo cerrado, claro y taxativo; en segundo lugar, con el terrorismo clásico no altera la base del injusto sino únicamente el mecanismo comisivo lo que podría generar que derivase en una duplicación peligrosista del tipo ya existente (artículo 343/344 del Código Penal).

Por todo lo anterior, la expansión razonable del TDig debe insertarse en una modalidad agravada del terrorismo tradicional a partir de la conservación de la unidad del bien jurídico e impulsar la coherencia sistemática y la previsibilidad normativa.

Por lo tanto, la modernización del derecho penal no significaría ampliar irreflexivamente el poder punitivo sino hacer un ajuste con sus transformaciones tecnológicas controlando el legislador y el juzgador, de manera que toda respuesta frente al TDig se encuentre dentro de los marcos de la legalidad, de la proporcionalidad, de la dignidad humana como centro del Estado Social de Derecho.

CONCLUSIONES

Durante el periodo comprendido entre 2020 a 2025, el tratamiento jurídico-penal del Terrorismo Digital (TDig) en Colombia no incorpora rasgos de la Teoría del Derecho Penal del Enemigo (TDPE) de Günter Jakobs.

La respuesta estatal, reflejada en las políticas públicas CONPES 3995 de 2020 y CONPES 4144 de 2025, pone en evidencia que se ha mantenido en una lógica preventiva y administrativa de gestión del riesgo, no en una expansión excepcional del poder punitivo ni en la construcción del "terrorista digital" como enemigo.

La noción de enemigo se disuelve en la figura del riesgo en tanto que el TDig queda subsumido en un fenómeno administrable más que punible; dado su atipicidad, el Estado no castiga al enemigo sino que lo previene, lo controla y lo regula. De ahí que Colombia no asuma el Derecho Penal del Enemigo, pero sí retenga su lógica anticipatoria, en ese nuevo modelo de gobernalidad digital.

El estudio pone de manifiesto, paralelamente, que Colombia no posee una regulación penal expresa, autónoma y sistemática del Terrorismo Digital (TDIG), de manera que sus manifestaciones

siguen ostentando un alto grado de atipicidad en la actualidad, pues no están recogidas integralmente en tipos penales específicos, ni constituyen una figura diferenciada dentro del sistema.

La ausencia normativa no es aséptica: pone de manifiesto contundentemente que el derecho penal clásico presenta limitaciones reales en relación con delitos desarrollados en escenarios virtuales, globales, descentralizados y tecnológicamente mediatizados; pero, ese vacío ni es ni puede ser un campo abonado para la importación del Derecho Penal del Enemigo como respuesta.

Dicho deslizamiento lleva a la erosión de los derechos fundamentales, pues se argumenta la restricción de libertades (privacidad, presunción de inocencia o libertad de expresión) en nombre de la seguridad , que acaba al final debilitando los derechos fundamentales y con ello el ESD amparado por la Constitución de 1991.

Sin embargo, la actual falta de tipo penal específico no quiere decir que el TDig esté fuera de la órbita del derecho penal. El estudio del artículo 343 del Código Penal, que protege la seguridad pública, permite afirmar que es jurídicamente posible una adecuación tecnológica del terrorismo clásico con la individualización del medio comisivo digital.

De allí, que tome relevancia la propuesta de Silva Sánchez(2001) en cuanto al garantismo activo: frente a los nuevos riesgos, el ordenamiento puede llegar a ampliar razonablemente su respuesta sin romper garantías; por lo tanto, la solución adecuada es el desarrollo agravante por el uso de medios digitales en el marco del terrorismo tradicional, no una nueva categoría delictual

En definitiva, se reproducen, los elementos constitutivos del terrorismo tradicional siguen reproduciéndose integralmente en el entorno digital, lo único que se transforma es su canal, un nuevo escenario de confrontación simbólica y operativa, pero con el mismo propósito de infundir terror y alterar los cimientos del pacto social.

Por consiguiente, el reto jurídico en Colombia no se localiza en la elaboración de un nuevo "terrorismo digital" como concepto autónomo, sino en adaptar el marco penal existente a las especificidades tecnológicas del fenómeno, sin renunciar a los principios constitucionales y garantistas que limitan el ejercicio del poder punitivo.

REFERENCIAS

Aramburú, I. J. M. (2015). Los enemigos de Jakobs. Revista Pensamiento Penal. https://www.pensamientopenal.com.ar/doctrina/40722-enemigos-jakobs

Bravo Peña, N. A. (2007). Derecho penal del enemigo: ¿Evolución o primitivismo del Derecho penal? Concepto doctrinal y jurídico, individualización y características del sujeto al que se le denomina enemigo [Memoria de licenciatura, Universidad de Chile, Facultad de Derecho]. Santiago de Chile.

Beck, U. (1986). La sociedad del riesgo: hacia una nueva modernidad. Paidós.

Cardeño, J. I. C. (2021). Sociedad Digital en Latinoamérica 2020-2021 : Un futuro posible de Colombia como sociedad digital. Una visión tecnoantropológica. In Research Portal Denmark (p. 321). Technical University of Denmark.

Castells, M. (2009). La era de la información: Economía, sociedad y cultura. Volumen I: La sociedad red (2.ª ed.). Madrid: Alianza Editorial.

Congreso de la República. (2009). Ley 1273 de 2009. Disponible en: https://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf

Congreso de la República de Colombia. (2000). Código Penal, Ley 599 de 2000. Disponible de http://www.secretariasenado.gov.co/senado/basedoc/ley_0599_2000.html

Consejo Nacional de Política Económica y Social (CONPES). (2025). *Política Nacional de Seguridad Digital y Ciberdefensa 2025–2030* (Documento CONPES 4144). Departamento Nacional de Planeación. https://colaboracion.dnp.gov.co/CDT/Conpes/Económicos/4144.pdf

Consejo Nacional de Política Económica y Social (CONPES). (2020). *Política Nacional de Confianza y Seguridad Digital* (Documento CONPES 3995). Departamento Nacional de Planeación. https://colaboracion.dnp.gov.co/CDT/Conpes/Económicos/3995.pdf

Consejo Nacional de Política Económica y Social (CONPES). (2016). *Política nacional de seguridad digital* (Documento CONPES 3854). Departamento Nacional de Planeación.https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf

Consejo Nacional de Política Económica y Social (CONPES). (2011). *Lineamientos de política para ciberseguridad y ciberdefensa* (Documento CONPES 3701). Departamento Nacional de Planeación. https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3701.pd

Corte Constitucional. (1995). Sala Plena. Sentencia C-038 del 9 de febrero de 1995. M.P.: Alejandro Martínez Caballero.

Corte Constitucional. (2012). Sala Plena. Sentencia C-365 del 16 de mayo de 2012. M.P.: Jorge Ignacio Pretelt Chaljub.

Corte Constitucional. (2019). Sala Plena. Sentencia C-233 del 29 de mayo de 2019. M.P.: Luis Guillermo Guerrero Pérez.

Dennig Dorothy. E. 2000. Cyberterrorism. Disponible en http://www. cs.georgetown.edu/~denning/ Consultado el 15.06.2015

El Espectador. (2025). Riesgos en línea: 78% de los colombianos ha sido víctima de amenazas digitales. ELESPECTADOR.COM. https://www.elespectador.com/tecnologia/riesgos-en-linea-78-de-los-colombianos-ha-sido-victima-de-amenazas-digitales/

Iftikhar, S. (2024). El ciberterrorismo como amenaza global: una revisión sobre sus repercusiones y contramedidas [Traducción propia de Cyberterrorism as a global threat: A review on repercussions and countermeasures]. PeerJ Computer Science, 10, 1772. https://doi.org/10.7717/peerj-cs.1772

INTERPOL. (2021). Guía nacional de estrategias contra el ciberdelito [Traducción propia de National cybercrime strategy guidebook]. INTERPOL. https://www.interpol.int/en/Crimes/Cybercrime

Hassemer, W. (1991). Persona, mundo y responsabilidad: Bases para una teoría de la imputación en derecho penal. Bogotá: Universidad Externado de Colombia.

Instituto Interregional de las Naciones Unidas para Investigaciones sobre la Delincuencia y la Justicia (UNICRI). (2020). Detener el virus de la desinformación: El riesgo del uso malicioso de las redes sociales durante la COVID-19 y las opciones tecnológicas para combatirlo. Naciones Unidas.

Jakobs, G. (2003). Derecho penal del ciudadano y Derecho penal del enemigo. En Jakobs/Cancio. Derecho penal del enemigo. (Trad. M Cancio Meliá). Madrid: Editorial Thomson Civitas.

Jakobs, G. (1996). Sociedad, norma y persona en la teoría de un Derecho penal funcional. Bogotá: Universidad Externado de Colombia.

Ferrajoli, L. (2001). Derecho y razón: teoría del garantismo penal. Trotta.

Francisco Agra, S. V. (2022). La digitalización del miedo: del terrorismo "clásico" al terrorismo "tecnológico". El Criminalista Digital. Papeles de Criminología, (10), 17-37. Universidad de Granada. ISSN 2340-6046.

Foucault, M. (2007). Seguridad, territorio, población: Conferencias en el Collège de France 1977–1978 (G. Burchell, Ed.; G. Burchell, Trad.). Palgrave Macmillan.

González Monguí, P. E. (2019). La negación de la calidad de ciudadano o de persona en el Derecho penal del enemigo. Opción: Revista de Ciencias Humanas y Sociales, 35(Especial No. 25), 1070–1103. Universidad del Zulia

Grabosky, P. (2001). Criminalidad virtual: Viejo vino en botellas nuevas [Traducción propia de Virtual criminality: Old wine in new bottles?]. Social & Legal Studies, 10(2), 243–249. https://doi.org/10.1177/09646390101000204Z

Mayer-Schönberger, V., & Cukier, K. (2013). Big data: A revolution that will transform how we live, work, and think. Houghton Mifflin Harcourt.

Mendoza Buergo, B. (2001). El derecho penal del enemigo: Análisis y crítica. Madrid: Civitas.

Poveda Criado, M. Á., & Torrente Barredo, B. (2016). Redes sociales y ciberterrorismo: Las TIC como herramienta terrorista. Opción, 32(8), 509–518. Universidad del Zulia. https://www.redalyc.org/pdf/310/31048481030.pdf

Organización de los Estados Americanos. (2002). Convención Interamericana contra el Terrorismo [Tratado]. OEA.

República de Colombia. (1991). Constitución Política de Colombia. Asamblea Nacional Constituyente. https://www.constitucioncolombia.com/

Rincón Romero, L. M. (2016). La permeabilización del derecho y las instituciones por los medios de comunicación: La incursión del derecho penal del enemigo. Misión Jurídica: Revista de Derecho y Ciencias Sociales, 11(julio–diciembre), 303–325.

Silva Sánchez, J.-M. (2001). La expansión del derecho penal: Aspectos de la política criminal en las sociedades postindustriales (2ª ed., revisada y ampliada). Civitas.

Timothy, T. (2003). Cyber terrorism: The new threat. Virginia: RAND Corporation.

Tuset Varela, D. (2024). Artificial intelligence law through the lens of Michel Foucault: Biopower, surveillance, and the reconfiguration of legal normativity [El derecho de la inteligencia artificial desde la perspectiva de Michel Foucault: Biopoder, vigilancia y reconfiguración de la normatividad jurídica]. Journal of Social Sciences. https://doi.org/10.4236/jss.2024.1212012

Wall, D. S. (2007). Ciberdelito: La transformación del crimen en la era de la información [Traducción propia de Cybercrime: The transformation of crime in the information age]. Polity Press.

Weimann, G. (2006). Terrorismo en Internet: La nueva arena, los nuevos desafíos [Traducción propia de Terror on the Internet: The new arena, the new challenges]. United States Institute of Peace Press.

Zeiger, S., & Gyte, J. (2020). The role of internet and social media use in radicalization processes [El papel del uso de internet y las redes sociales en los procesos de radicalización] [Traducción propia]. En Extremism and online radicalization. Hedayah Center.

Zuboff, S. (2019). La era del capitalismo de la vigilancia. Paidós.

KAROL VALENTINA CHAVES PRIETO <kchaves@universidadmayor.edu.co>

Entrega de guía y matriz de apoyo – Derecho Penal del Enemigo

KAROL VALENTINA CHAVES PRIETO <kchaves@universidadmayor.edu.co> 4 de diciembre de 2025 a las 16:08

Para: Consultorio Jurídico - Derecho - Universidad - <consultoriojuridico@universidadmayor.edu.co>, Jairo Borja Medina <jborjam@universidadmayor.edu.co>

Estimados(as) integrantes del Consultorio Jurídico
Facultad de Derecho – Universidad Colegio Mayor de Cundinamarca:

Reciban un cordial saludo.

Por medio de la presente me permito hacer entrega formal de la Guía sobre Derecho Penal del Enemigo, producto de mi proceso investigativo en la Maestría en Derecho Penal de esta Facultad y derivada de la tesis titulada “Terrorismo digital desde la perspectiva del Derecho Penal del Enemigo (2020–2025)”. En esta ocasión, les remito el desarrollo específico relativo a la teoría del Derecho Penal del Enemigo, junto con los insumos construidos para su estudio y aplicación académica.

La guía se acompaña de la matriz de apoyo incorporada en el documento y de su enlace de acceso, con el fin de que estos materiales puedan ser compartidos con el estudiantado cuando el Consultorio lo considere pertinente:

Enlace de la matriz:

https://docs.google.com/spreadsheets/d/1iOI6dUN6RR9xWH8HnKCkNVDx_oiGXptHM8rkKq75NhI/edit?usp=drivesdk

El propósito central de esta entrega es que, a partir de la guía y la matriz, se cuente con una base que permita identificar los parámetros y rasgos característicos de la teoría del Derecho Penal del Enemigo en relación con disposiciones normativas concretas, facilitando su lectura crítica y su reconocimiento en el análisis jurídico. Con ello, se busca abrir camino para el estudio y desarrollo de estos elementos desde una perspectiva propia del Estado Social de Derecho, valorando sus tensiones, límites y alcances dentro del marco constitucional.

Agradezco su atención y la recepción de este material.

Quedo atenta a cualquier comentario, observación o recomendación que consideren oportunos.

Cordialmente,

Karol Valentina Chaves Prieto.

Maestranda en Derecho Penal

Facultad de Derecho – Universidad Colegio Mayor de Cundinamarca

GUIA DEREHO PENAL DEL ENEMIGO UCMC.pdf
3957K

Derecho Penal del Enemigo: guía de estudio y análisis para estudiantes de Consultorio Jurídico Facultad de Derecho. Universidad Colegio Mayor de Cundinamarca

Karol Valentina Chaves Prieto.
Universidad Colegio Mayor de Cundinamarca
Maestría en Derecho Penal
2025

TABLA DE CONTENIDO

Introducción

El Derecho Penal del Enemigo (DPE), es una de las teorías del Derecho Penal más debatidas en la actualidad porque propone una respuesta estatal diferenciada y desigual frente a ciertos sujetos que son calificados como especialmente peligrosos.

Esta categoría, que ha sido expuesta principalmente por Günther Jakobs desde el funcionalismo sistémico, intenta establecer que el Derecho Penal no sanciona solamente hechos, sino que al mismo tiempo protege la vigencia de las normas que permiten la vida en sociedad.

En esta idea, no todos los sujetos (al desobedecer la ley) están ubicados dentro del mismo plano: en primer lugar, algunos de esos sujetos seguirán siendo ciudadanos conservando su estatuto de sujeto de derechos, aun cuando ellos pudieran delinquir; por el contrario, otros, "individuos" que enlazan su comportamiento delictivo con una conducta reiterativa, organizada o radicalmente opuesta al orden jurídico, serán considerados sujetos que se autoexcluyen del pacto social, bajo la categoría de -no persona-.

Dichas características originan tensiones en relación con los principios del Estado Social de Derecho, en particular con la dignidad humana, la igualdad, y el debido proceso.

Esta guía, busca que el estudiantado comprenda y realice una lectura critica de la Teoría del Derecho Penal del Enemigo (TDPE) especialmente en relación con sus rasgos característicos y sus implicaciones en la práctica penal contemporánea; de este modo, se espera que pueda verificar en qué punto una norma se aproxima a una lógica de "enemigo" y que cuente con criterios claros para interpretar, de forma argumentada, casos o discursos penales actuales.

Objetivos.

Objetivo general

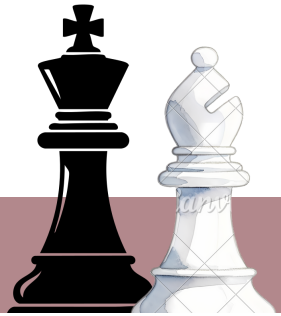
Orientar al estudiantado en la comprensión y lectura crítica de la Teoría del Derecho Penal del Enemigo (TDPE), a partir de sus rasgos y de sus implicaciones en la práctica penal contemporánea.

Objetivos específicos

- Reconocer los fundamentos teóricos centrales de la TDPE, diferenciándolos de los postulados del Derecho Penal del Ciudadano.

- Analizar las implicaciones de la TDPE en la normatividad penal contemporánea, especialmente frente al Estado Social de Derecho.

- Socializar la matriz previamente elaborada sobre la TDPE, con el propósito de orientar su uso para identificar su presencia en la normatividad penal vigente.



Metodología

El enfoque que define la presente guía se inscribe en un diseño jurídico-analítico de carácter hermenéutico y documental, orientado a la comprensión e interpretación crítica de la Teoría del Derecho Penal del Enemigo (TDPE), a partir de su tratamiento en diferentes fuentes normativas, doctrinales y jurisprudenciales.

De acuerdo con Sepúlveda López y Solano de Jinete (2008) esta investigación persigue la reconstrucción de categorías teóricas, su contraste con la normatividad existente y la generación de criterios interpretativos exigentes, antes que la vía del procedimiento empírico cuantitativo.

La guía, en consecuencia, se lanza por una senda metodológica cualitativa, que articula la lectura sistemática del material jurídico con su valoración crítica, con el fin de analizar la presencia de lógicas de "enemigo" en la época actual del derecho penal.

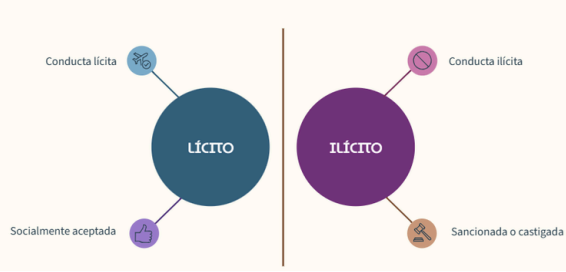
Fundamentos básicos del Derecho Penal en Gunter Jakobs

El funcionalismo en Jakobs se construye desde el funcionalismo sistémico inspirado en la teoría de los sistemas de Niklas Luhmann. Bajo esta mirada, la sociedad se concibe como un sistema complejo compuesto por subsistemas autónomos (familia, economía, política, derecho, etc.), que operan mediante sus propios códigos de comunicación para garantizar estabilidad y continuidad social.

Luhmann concibe la sociedad como un gran organismo donde cada subsistema cumple una función específica. El Derecho opera de manera autónoma con su propio código binario, creando expectativas normativas estables que reducen la incertidumbre social.

Conceptos Claves del Sistema Jurídico

- **Autorreferencia**: El sistema se diferencia de su entorno; sabe qué le pertenece y qué no.
- **Autopoiesis:** El sistema produce sus propios elementos (normas, decisiones, etc.).
- **Código Binario:** Opera bajo la distinción fundamental: Lícito / Ilícito.
- **Función Social:** Reducir la incertidumbre social, creando expectativas estables.



Fuente: Elaboración propia.

El Derecho opera con una lógica interna y terminología específica.

No necesita recurrir a valores religiosos, morales o políticos

No se condena a alguien por "ser malo", sino por cometer un acto ilícito según una norma jurídica.

Günther Jakobs: El Derecho Penal como Garante de la Norma

Jakobs retoma la base funcionalista de Luhmann y la traslada al Derecho Penal, por lo que ese código se convierte en:

Conducta conforme al Derecho	Conducta que se aparta del Derecho

Desde esta perspectiva, el Derecho Penal no protege directamente bienes jurídicos (como la vida o la propiedad), sino que su función primordial es garantizar la vigencia de las normas que los sustentan.

Cuando una persona infringe el Derecho, el sistema penal reacciona para estabilizar las expectativas sociales y restaurar el equilibrio que ha sido alterado.

Para Jakobs, la pena no es venganza ni castigo moral; en cambio, es una forma de comunicación simbólica: el lenguaje mediante el cual el Estado reafirma el orden social.

Cada vez que el Estado castiga, le dice a la sociedad: tranquilos, la norma sigue viva; pueden seguir confiando en el sistema.

De esta manera, el Derecho Penal cumple dos grandes funciones:

Prevención

El Derecho Penal actúa preventivamente para evitar nuevas defraudaciones de la norma, manteniendo la previsibilidad del comportamiento social; esta prevención se proyecta tanto hacia la sociedad en general como hacia el autor concreto, con el fin de impedir futuras negaciones del orden jurídico.

Estabilización

El Derecho Penal reafirma la vigencia de la norma cuando un delito la ha puesto en duda, restableciendo la confianza colectiva en el sistema jurídico y garantizando la continuidad del orden social.

Fuente: Elaboración propia con base en Jakobs (2003)

La Misión del Derecho Penal según Jakobs

En esa perspectiva, la sociedad existe y se sostiene porque comparte expectativas normativas estables sobre el comportamiento; cada individuo ocupa roles sociales que refuerzan esas expectativas y, cuando alguien abandona su rol o actúa contra la norma, defrauda la expectativa normativa y pone en riesgo la estabilidad del sistema.

Por eso, para Jakobs el delito no se define ante todo como lesión de un bien jurídico, sino como una "comunicación defectuosa" que niega la norma y rompe la confianza social en su obligatoriedad

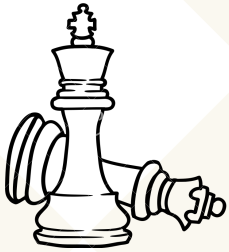
En coherencia con ello, la pena no se justifica por un criterio moral o retributivo, sino porque restaura la vigencia de la norma negada; en otras palabras, La pena es el idioma con el que el Derecho se comunica con la sociedad.

De acuerdo, con el doctrinante Alejandro Sánchez González (2009) estima que para Jakobs la pena es una respuesta institucional ante la infracción de una norma "y, mediante ella, se pone de manifiesto que ha de conservarse la fidelidad al derecho, a consta del infractor responsable .De esta forma, la misión dela pena consiste en el mantenimiento de la norma, como modelo de orientación para los contactos sociales" (p.199)

La misión del Derecho Penal, entonces, es estabilizar la confianza normativa y evitar la anomia (falta de reglas). Se trata de un Derecho Penal preventivo y funcional, no retributivo. Ejemplo:

Fuente: Elaboración propia .

Persona y Apoyo Cognitivo



Para Günther Jakobs la persona no se define por la sola condición humana, sino por su estatus normativo dentro del sistema: se es persona conforme se sirva a la sociedad, y es la norma la que reconoce al individuo como tal, exigiendo una contraprestación mínima consistente en la manifestación cognitiva de la voluntad de comportarse conforme a las reglas sociales.

Esa contraprestación es lo que el jurista llama apoyo cognitivo o seguridad cognitiva mínima: el sistema solo puede tratar a alguien como persona/ciudadano si puede esperar razonablemente que actuará conforme al Derecho en el futuro

Cuando un sujeto niega consciente y persistentemente el carácter vinculante del orden normativo, “deja de ofrecer la certeza cognitiva de que se comporta como persona” y el sistema ya no lo reconoce como ciudadano, sino como enemigo.

Persona Jurídica

Cumple roles sociales previsibles: trabajador, padre, ciudadano. Ofrece apoyo cognitivo al sistema.

Los demás pueden confiar en que actuará dentro de lo esperado.

Ruptura del Vínculo

Cuando niega la norma de manera total y permanente, pierde el estatus de persona jurídica.

No Persona

Se convierte en fuente de peligro. El sistema ya no dialoga, se defiende.

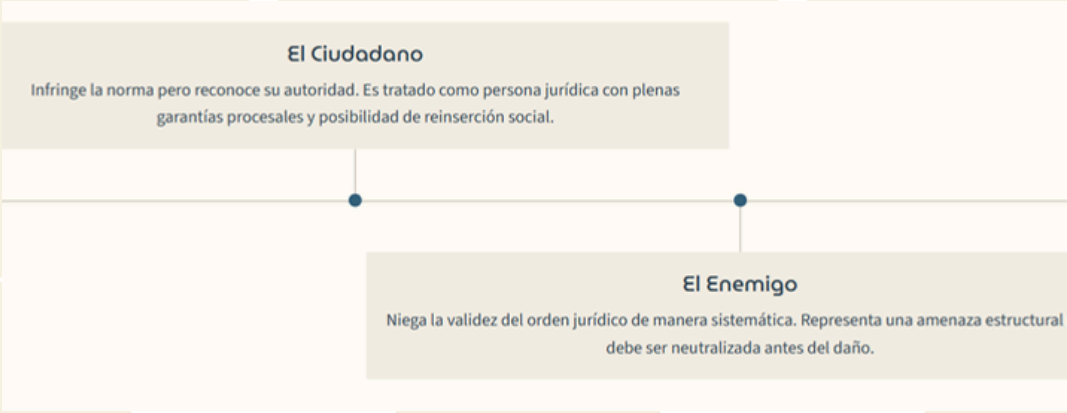
Fuente: Elaboración propia con base en Jakobs (2003)

Derecho Penal del Ciudadano vs Derecho Penal del Enemigo

La distinción entre Derecho Penal del Ciudadano y Derecho Penal del Enemigo surge directamente de la forma en que Jakobs concibe a la persona: solo es persona quien ofrece al sistema una seguridad cognitiva mínima de que actuará conforme al Derecho, es decir, quien sostiene expectativas normativas básicas

En ese marco, el Derecho Penal del Ciudadano es el que se aplica a quien delinque sin romper definitivamente su vínculo con el sistema: la persona sigue siendo reconocida como sujeto de derechos, conserva garantías plenas y la pena funciona como comunicación normativa que reprocha el hecho cometido y reafirma la vigencia de la norma frente a toda la sociedad

En cambio, la Teoría Derecho Penal del Enemigo, en adelante TDPE, es un conjunto de normas excepcionales dirigido a quienes se han apartado de forma duradera del Derecho y no reconocen su obligatoriedad; frente a ellos ya no se busca mantener expectativas normativas —porque no hay confianza posible— sino neutralizar un peligro futuro, lo que explica la anticipación punitiva, el derecho penal del autor y la reducción de garantías.

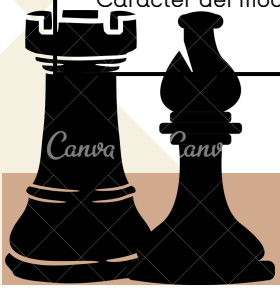


Fuente: Elaboración propia con base en Jakobs (2003)

03. Derecho Penal del Ciudadano vs Derecho Penal del Enemigo

Criterio	Derecho Penal del Ciudadano	Derecho Penal del Enemigo
Destinatario	Persona que infringe la norma pero no rompe de forma definitiva el pacto social; sigue siendo ciudadano.	Individuo que se aparta de manera duradera del Derecho y niega el orden jurídico; es tratado como enemigo.
Relación con el sistema	Mantiene un vínculo con el sistema jurídico y puede ser reconducido a la normalidad normativa.	Se considera que ha perdido la "seguridad cognitiva mínima"; deja de ser interlocutor y pasa a ser fuente de riesgo.
Finalidad de la pena	Reafirmar la vigencia de la norma y restaurar la confianza en el orden jurídico frente al hecho cometido.	Neutralizar un peligro futuro; la intervención se dirige a evitar amenazas, no a reprochar el pasado.
Lógica del castigo	Derecho penal comunicativo y garantista: castiga hechos dentro de límites constitucionales.	Derecho penal preventivo y peligrosista: prioriza la defensa del sistema frente al riesgo.
Momento de intervención	Reacciona ante hechos consumados.	Anticipa la punibilidad: sanciona fases tempranas o preparatorias.
Centro del reproche	El hecho concreto cometido por el ciudadano.	La peligrosidad del autor, su rol o pertenencia (derecho penal del autor).
Garantías procesales	Conserva garantías plenas: debido proceso, presunción de inocencia, proporcionalidad.	Se flexibilizan o reducen garantías por considerarse que no es ciudadano pleno.
Tipo de coacción estatal	Pena orientada a reafirmar norma y mantener integración social.	Medidas orientadas a contención, aseguramiento o exclusión del peligro.
Carácter del modelo	Regla general dentro del Estado de Derecho.	Excepcional, reservado a amenazas estructurales o extremas.

Fuente: Elaboración propia con base en Jakobs (2003)



Principios del Derecho Penal del Enemigo

1 Dicotomía entre ciudadano y enemigo

Sustentado en el trato desigual que deriva en sus destinatarios: por su parte el ciudadano "persona" que reconoce la validez del orden social, aunque cometa delitos; y el enemigo "no persona" que niega ese orden de manera sistema y persistente, considerado una amenaza a neutralizar.

2 Funcionalismo Sistémico

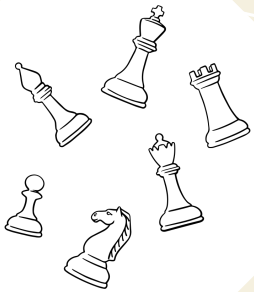
Derecho Penal como instrumento de estabilización de expectativas normativas donde se prevé la prevalencia del orden social sobre la protección de derechos individuales.

3 Derecho Penal del autor

Implica que la persona es penalizada no por su actuar, sino por quien es. Existe un desplazamiento hacia la prevención castigando a sujetos con conductas o perfiles considerados amenazantes, incluso antes de efectuar algún actuar delictivo.

4 Anticipación de la punibilidad.

Sancionar conductas en fases muy tempranas, por la potencialidad del riesgo frente al pacto social, llegando a sancionar etapas preparatoria o de simple sospecha.



Principios del Derecho Penal del Enemigo

5 Reducción de garantías procesales

El enemigo al no ser persona dentro del Derecho Penal, no puede ser juzgado bajo las misma condiciones que el ciudadano común, por lo que se reducen o restringen derecho fundamentales como la presunción de inocencia, el debido proceso y la libertad personal, entre otras garantías.

6 Neutralización de amenazas

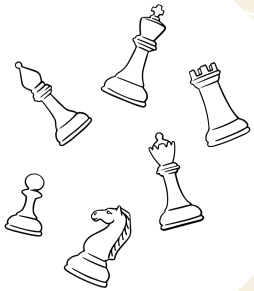
El enemigo puede destruir el pacto social, este debe ser contenido o eliminado en su defecto antes de que logre actuar.

7 Despersonalización del individuo

Deriva de la categoría de "no persona" determinada por la norma genera una pérdida de la dignidad humana del individuo y pasa a ser tratado como un objeto de riesgo.

8 Aplicación excepcional

Concurre con contextos históricos donde se activa para hacer frente a amenazas extraordinarias que el propio ordenamiento identifica.



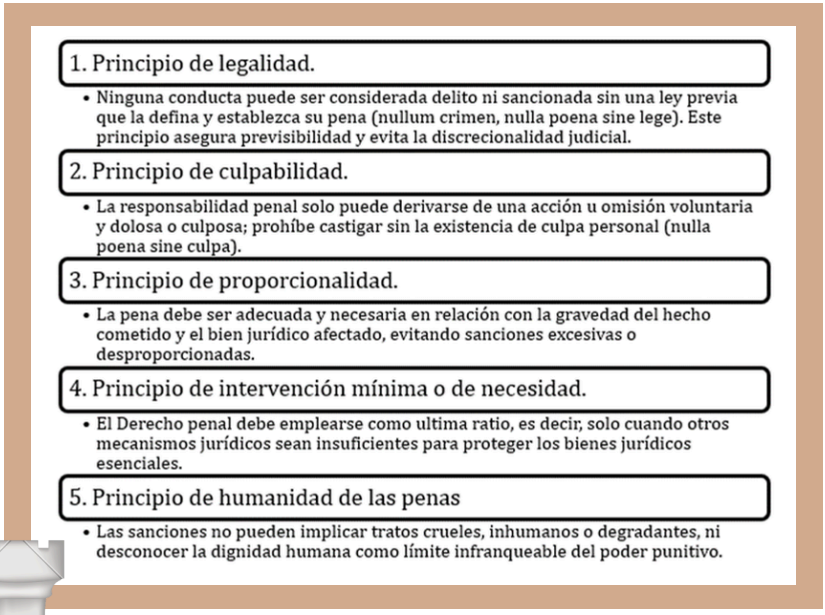
Críticas y tensiones frente al Estado Social de Derecho en Colombia.

La Constitución de 1991 identifica a Colombia como un Estado Social de Derecho desde ahora ESD, basado en la dignidad humana, el trabajo, la solidaridad y el interés general. Ese punto de partida no es solo un tema de enunciación, sino que introduce una variación en la forma de entender al Estado, que ha de ser entendido como al servicio de la persona, lo cual explica que todo el derecho - sobre todo el penal - queda afectado por la Constitución.

Dicho de otra manera, el ius puniendi ya no puede moverse con libertad, sino que ha de quedar determinado por principios, valores y derechos fundamentales que establece la propia Constitución. Así, el derecho penal no encuentra su fundamento en sí mismo, sino sólo en el hecho de que protege bienes jurídicos y garantías, pero no porque funcione como una mera herramienta de control o exclusión.

Su uso ha de ser racional y limitado, en forma de ultima ratio: ha de funcionar sólo cuando otras formas de respuestas no son suficientes y el daño o riesgo es realmente grave. Esta forma de entenderlo se relaciona también con el garantismo penal de Ferrajoli: la pena tiene sentido sólo si es estrictamente necesaria para asegurar derechos y al mismo tiempo para evitar excesos del poder punitivo del Estado.

Finalmente, ese garantismo se caracteriza por los límites materiales al ius puniendi:



Fuente: Elaboración propia con base en Ferrajoli, L. (1995).

Fuente: Elaboración propia.

Bajo esta perspectiva, es previsible que la visión garantista que contempla el Estado Social de Derecho (ESD) derive en un conflicto claro frente a los fundamentos de la TDPE de Gunter Jakobs.

La propuesta de Jakobs plantea dos derechos penales que coexisten en el desarrollo cotidiano del Estado: ciudadano y el del enemigo.

En cuanto al Derecho Penal del ciudadano, es una categoría de aplicación clásica donde el que infringe la norma sigue siendo tratado como persona, pues no ha quebrantado el pacto social o abandonado las reglas mínimas de convivencia, en consecuencia, solo basta la pena para reafirmar la norma frente a la sociedad.

En este Derecho Penal, se mantienen las garantías del Derecho Penal tradicional, no existe per se, algún fundamento en contrario que permita concluir lo contrario; por esta razón, en este sistema jurídico los principios del ESD se mantienen incólumes.

Ahora bien, no es posible afirmar lo mismo del Derecho Penal del Enemigo (DPE), propuesto como segunda categoría, frente aquellas-no personas- estos son: aquellos individuos que significan una amenaza permanente para el pacto social, pues no solo solo infringe las normas, sino que busca desaparecer la validez del sistema jurídico-político en su totalidad, siendo insuficiente el Derecho Penal del ciudadano para su tratamiento.

Cómo se Erosionan los Principios Constitucionales

DIGNIDAD HUMANA

ESD: Todos los seres humanos la poseen por igual, incluso el delincuente

DPE: Solo la conserva quien coopera con el sistema; el "enemigo" la pierde

Consecuencia: Se justifica la despersonalización

IGUALDAD ANTE LA LEY

ESD: Toda persona tiene los mismos derechos procesales

DPE: Se divide la sociedad entre ciudadanos y enemigos

Consecuencia: Se rompe la universalidad del Derecho

CULPABILIDAD

ESD: Se castigan actos probados, no identidades

DPE: Se castiga la "peligrosidad" o intención futura

Consecuencia: Aparece el castigo preventivo

PROPORCIONALIDAD

ESD: La pena busca equilibrio entre daño y sanción

DPE: La pena se justifica por seguridad, no por justicia

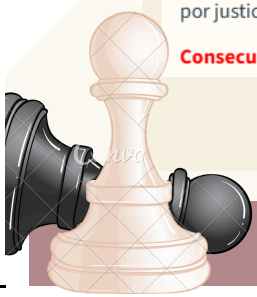
Consecuencia: Se amplía el poder punitivo

HUMANIDAD DE LA PENA

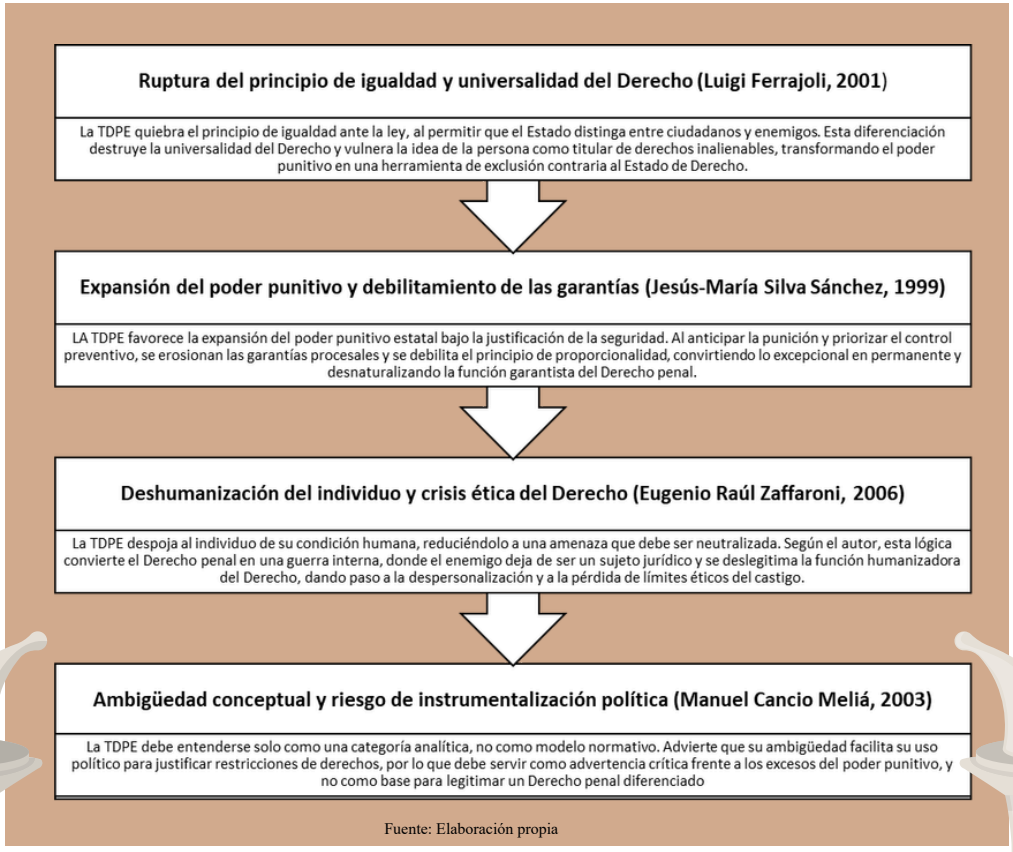
ESD: La sanción respeta la dignidad del condenado

DPE: Se aceptan medidas inhumanas para "neutralizar peligros"

Consecuencia: Se erosiona el debido proceso



Criticas al Derecho Penal del Enemigo



Fuente: Elaboración propia

En conjunto, esas críticas no solo cuestionan la legitimidad del modelo de Jakobs, sino que reafirman la necesidad de un Derecho Penal garantista capaz de responder a los desafíos contemporáneos sin renunciar a su esencia: la dignidad humana y la vigencia universal de la ley.

MATRIZ

Para ilustrar su aplicación, la guía retoma los análisis previamente realizados en la investigación sobre los documentos CONPES 3995 de 2020 y CONPES 4144 de 2025, con el fin de observar comparativamente el alcance e intensidad de estos rasgos en el periodo estudiado.

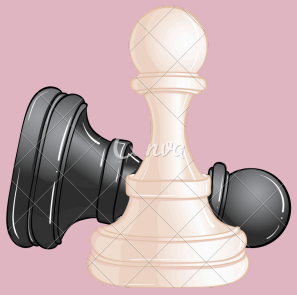
En esta guía se presentan los resultados del trabajo de investigación titulado “Terrorismo Digital en Colombia desde la perspectiva del Derecho Penal del Enemigo (2024–2025)”.

A partir del desarrollo teórico aquí expuesto, se incorpora una matriz de identificación, sistematizada en formato Excel, que permite contrastar la normatividad y los lineamientos institucionales con los criterios propios del Derecho Penal del Enemigo analizados en la guía.

Esta herramienta hace posible evaluar, desde un enfoque cuantitativo y cualitativo, en qué medida una disposición normativa o política estatal puede aproximarse a una lógica de “enemigo” —según los rasgos definidos por Jakobs— o si, por el contrario, se mantiene dentro del marco garantista del Estado Social de Derecho

Finalmente, para consultar la matriz en su versión completa, junto con sus instrucciones de uso, se remite y comparte el siguiente enlace, a través del cual podrán acceder al documento íntegro.

https://docs.google.com/spreadsheets/d/1iOI6dUN6RR9xWH8HnKCkNVDx_oiGXptHM8rkKq75NhI/edit?usp=sharing



Conclusiones

1. La guía permite comprender la TDPE como una teoría excepcional que se activa cuando el Estado identifica sujetos que rompen de forma duradera el orden jurídico y son tratados como riesgos.
2. Desde Jakobs, la diferencia ciudadano/enemigo depende del concepto funcional de persona: solo quien mantiene "apoyo cognitivo" es reconocido plenamente como ciudadano ante el Derecho Penal.
3. El Derecho Penal del Ciudadano mantiene garantías y reprocha hechos, mientras que el Derecho Penal del Enemigo anticipa la intervención, flexibiliza garantías y busca neutralizar peligros futuros.
4. Los rasgos estructurales del enemigo (derecho penal de autor, anticipación punitiva, restricción de garantías y neutralización) sirven como criterios claros para detectar desplazamientos punitivos en la normatividad vigente.
5. La matriz incluida en esta guía traduce esos criterios a un instrumento técnico cuantitativo-cualitativo, facilitando verificar si una norma o política se acerca a una lógica de enemigo o permanece dentro del Estado Social de Derecho.
6. La aplicación ejemplificada con los CONPES 3909 de 2020 y 4144 de 2025 muestra cómo esta herramienta permite evaluar críticamente el tratamiento institucional del Terrorismo Digital en Colombia durante 2024–2025.

Referencias.

Ferrajoli, L. (1995). Derecho y razón: Teoría del garantismo penal. Madrid: Trotta.

Jakobs, G. (2003). Derecho penal del ciudadano y Derecho penal del enemigo. En Jakobs/Cancio. Derecho penal del enemigo. (Trad. M Cancio Meliá). Madrid: Editorial Thomson Civitas.

Jakobs, G. (2007). ¿Derecho Penal del enemigo? Un estudio acerca de los presupuestos de la juridicidad. En Jakobs/Polaino Navarrete, Las condiciones de juridicidad del sistema penal (pp. 17–44). Lima: Editorial Grijley.

República de Colombia. (1991). Constitución Política de Colombia. Asamblea Nacional Constituyente. https://www.constitucioncolombia.com/

Sánchez González, A. (2009). Luhmann, Jakobs y el Derecho Penal del enemigo. Revista Crítica Jurídica, (28), 1–20.

Solano de Jinete, N., & Sepúlveda López, M. (2008). Metodología de la investigación social y jurídica (1.ª ed.). Grupo Editorial Ibáñez.

Zaffaroni, E. R. (2011). El enemigo en el Derecho Penal. Coyoacán.

PROYECTO DE LEY N.°____ DE 2025

“POR MEDIO DE LA CUAL SE RECONOCE EL USO DE MEDIOS DIGITALES COMO MODALIDAD AGRAVADA DEL TERRORISMO Y SE MODIFICA EL ARTÍCULO 344 DEL CÓDIGO PENAL COLOMBIANO.”

Bogotá D.C, _____2026

Doctor:

Diego Alejandro González

Secretario General del Senado de la República.

Asunto: Radicación Proyecto de Ley “Por medio de la cual se reconoce el uso de medios digitales como modalidad agravada del terrorismo y se modifica el artículo 344 del Código Penal colombiano.”

De manera atenta y respetuosa y en consideración a los artículos 139 y 140 de la Ley 5 de 1992 presenta a consideración del Senado de la República el Proyecto de “Por medio de la cual se reconoce el uso de medios digitales como modalidad agravada del terrorismo y se modifica el artículo 344 del Código Penal colombiano.”

Iniciativa legislativa que cumple con las disposiciones correspondientes al orden de redacción consagrado en el artículo 145 de la citada Ley.

Agradezco disponer el trámite legislativo previsto en el artículo 144 de la Ley 5 de 1992 respecto del siguiente proyecto

Cordialmente.

PROYECTO DE LEY N.°____ DE 2025

“POR MEDIO DE LA CUAL SE RECONOCE EL USO DE MEDIOS DIGITALES COMO MODALIDAD AGRAVADA DEL TERRORISMO Y SE MODIFICA EL ARTÍCULO 344 DEL CÓDIGO PENAL COLOMBIANO.”

EL CONGRESO DE COLOMBIA
DECRETA:

Artículo 1°. Objeto de la ley. La presente ley tiene por objeto fortalecer la respuesta penal frente al terrorismo cuando sea realizado mediante medios digitales o tecnológicos de información y comunicaciones, en tanto dichos medios incrementan el peligro concreto contra la seguridad pública, cuya manifestación contemporánea incluye su dimensión digital, garantizando la armonía con la Constitución y los derechos humanos.

Artículo 2°. Definición de medios digitales para efectos penales. Para efectos del numeral 9 del artículo 344, entiéndase por medios digitales el uso de redes, sistemas, plataformas, servicios o tecnologías de información y comunicación —incluidas redes sociales, mensajería digital, sistemas informáticos, herramientas automatizadas o algorítmicas— que permitan:

a) Difundir masivamente amenazas idóneas para crear o mantener zozobra o terror en la población;
b) Coordinar, facilitar o amplificar actos con finalidad terrorista;
c) Manipular o instrumentalizar entornos digitales con el propósito de generar intimidación colectiva o coacción a autoridades o a la sociedad.

Parágrafo. En ningún caso se considerará medio digital la mera expresión de opinión, crítica, protesta social pacífica o ejercicio legítimo de libertad de expresión sin finalidad terrorista, aun cuando se realice en plataformas digitales.

Artículo 3°. Modifíquese el articulo 344 de la Ley 599 del 2000-Código Penal Colombiano_ y adiciónese un numeral el cual quedara así:

Artículo 344. Circunstancias de agravación punitiva. Las penas señaladas en el inciso primero del artículo anterior, serán de ciento noventa y dos (192) a trescientos sesenta (360) meses de prisión y multa de seis mil seiscientos sesenta y seis punto sesenta y seis (6.6666.66) a cuarenta y cinco mil (45.000) salarios mínimos legales mensuales vigentes, cuando:

(…)

6. La conducta se ejecute mediante medios digitales o tecnológicos de información y comunicaciones, con finalidad terrorista.

Artículo 4°. No procedencia. El agravante del numeral 6 del artículo 344 de la Ley 599 de 2000, no procederá cuando el hecho digital se subsuma íntegramente en otro tipo penal sin diferenciación frente al terrorismo; en tal caso se aplicará únicamente el tipo correspondiente, sin duplicidad punitiva.

Articulo 5°. Vigencia y derogatorias. La presente ley rige a partir de su sanción, promulgación y publicación en el Diario Oficial y deroga las disposiciones que le sean contrarias.

PROYECTO DE LEY N.°____ DE 2025

“POR MEDIO DE LA CUAL SE RECONOCE EL USO DE MEDIOS DIGITALES COMO MODALIDAD AGRAVADA DEL TERRORISMO Y SE MODIFICA EL ARTÍCULO 344 DEL CÓDIGO PENAL COLOMBIANO.”

EXPOSICIÓN DE MOTIVOS.

El desarrollo acelerado de las Tecnologías de la Información y las Comunicaciones (TIC) ha ampliado el campo de interacción social hacia escenarios no físicos, configurando el ciberespacio como un entorno cotidiano de comunicación, intercambio de datos y producción de sentido colectivo.

Este proceso, intensificado desde la pandemia de COVID-19, incrementó la dependencia social e institucional de los medios digitales y abrió nuevas oportunidades para actores violentos que instrumentalizan tales entornos.

Proporción de personas que utilizan internet en 2023.

DEPARTAMENTO	Total nacional (%)	Cabecera (%)	Centros poblados y rural disperso (%)
Total nacional	**77,3**	**82,6**	**59,6**
Amazonas	39,3	49,6	28,0
Antioquia	80,9	83,7	68,7
Arauca	66,0	78,1	42,9
Atlántico	80,6	81,3	68,0
Bogotá, D.C.	85,9	85,9	78,4
Bolívar	69,2	74,8	53,6
Boyacá	67,9	76,6	54,1
Caldas	76,6	81,7	59,0
Caquetá	72,3	74,7	67,5
Casanare	75,8	83,0	56,4
Cauca	65,9	79,5	58,2
Cesar	75,0	79,6	60,6
Chocó	43,4	66,2	25,7
Córdoba	67,5	77,0	57,1
Cundinamarca	83,5	86,2	74,6
Guainía	53,6	68,3	40,0
Guaviare	71,8	78,8	62,3
Huila	77,5	81,5	71,5
La Guajira	52,6	71,2	33,4
Magdalena	72,1	77,3	60,5
Meta	86,7	89,4	78,2
Nariño	66,0	77,8	56,6
Norte de Santander	74,4	78,7	57,2
Putumayo	59,4	71,6	45,7
Quindío	80,6	81,5	73,6
Risaralda	78,5	82,9	60,2
San Andrés	68,8	68,8	*
Santander	80,9	87,1	58,8
Sucre	66,8	76,1	51,7
Tolima	76,2	81,5	63,9
Valle del Cauca	84,7	86,1	76,1
Vaupés	34,1	66,4	20,5
Vichada	14,5	51,1	2,7

Fuente: Tomada del Departamento Administrativo Nacional de Estadística, 2023, Encuesta de Calidad de Vida- ECV (p.12)

En el caso colombiano, este incremento se deja ver con claridad ya que en 2023 “un 77,3% de las personas de cinco años y más usó Internet (82,6% en cabeceras y 59,6% en zonas rurales), mientras que en 2022 el total se situó en 72,8% (78,9% en cabeceras y un 52,6% en centros poblados y rural disperso” (DANE, 2023, p.13).

Estas cifras evidencian un incremento sostenido en el despliegue digital, a la vez que amplía los ámbitos de acción potencial de las estructuras ilícitas en el ciberespacio, aumentando los desafíos del Estado en lo que toca a la prevención, control y regulación de actividades terroristas en línea.

El Instituto de Investigación Interregional sobre Crimen y Justicia de las Naciones Unidas (UNICRI), en su informe de 2020, ha destacado:

La desinformación y la información errónea en las redes sociales no son problemas nuevos, pero la crisis de la COVID-19 los ha amplificado y ha creado nuevas oportunidades para actores no estatales violentos. En los últimos meses hemos visto numerosos casos de uso malintencionado de las redes sociales, para socavar la confianza en los gobiernos y, al mismo tiempo, reforzar las narrativas extremistas y las estrategias de reclutamiento. (p.5).

En igual sentido, Jürgen Stock, Secretario General de INTERPOL señaló que “esta coyuntura especial ha sido aprovechada por los grupos cibercriminales para acelerar sus campañas de dispersión de malware, el compromiso de data sensible en las organizaciones, facilitar las estafas en Internet y la desinformación” (Bautista, 2020, p. 4)

A nivel nacional, el periódico el Espectador (2025) en su artículo establece que más del 78% ha sido víctima de amenazas digitales entre las principales se encuentran:

(…) la desinformación (59 %), la exposición a contenidos violentos (47 %) y el discurso de odio (39 %). Además, el estudio alerta sobre un fenómeno preocupante: la creación de deepfakes de contenido pornográfico, una práctica que afecta al 20 % de los encuestados en Colombia, posicionando como el segundo país con mayor incidencia de este problema.

Estos datos reflejan, que los grupos terroristas han evolucionado para adaptarse a esta nueva era representando una mayor amenaza estatal en el anonimato, incitando la violencia, coordinando ataques, difundiendo discursos que afectan a la seguridad del Estado y sus

ciudadanos, lo cual, demanda una respuesta eficaz ante las vulnerabilidades del ecosistema virtual.

El Instituto de Investigación Interregional sobre Crimen y Justicia de las Naciones Unidas (UNICRI), en su informe de 2020, ha destacado:

> La desinformación y la información errónea en las redes sociales no son problemas nuevos, pero la crisis de la COVID-19 los ha amplificado y ha creado nuevas oportunidades para actores no estatales violentos. En los últimos meses hemos visto numerosos casos de uso malintencionado de las redes sociales, para socavar la confianza en los gobiernos y, al mismo tiempo, reforzar las narrativas extremistas y las estrategias de reclutamiento. (p.5).

En igual sentido, Jürgen Stock, Secretario General de INTERPOL señaló que "esta coyuntura especial ha sido aprovechada por los grupos cibercriminales para acelerar sus campañas de dispersión de malware, el compromiso de data sensible en las organizaciones, facilitar las estafas en Internet y la desinformación" (Bautista, 2020, p. 4)

A nivel nacional, el periódico el Espectador (2025) en su artículo establece que más del 78% ha sido víctima de amenazas digitales entre las principales se encuentran:

> (…) la desinformación (59 %), la exposición a contenidos violentos (47 %) y el discurso de odio (39 %). Además, el estudio alerta sobre un fenómeno preocupante: la creación de deepfakes de contenido pornográfico, una práctica que afecta al 20 % de los encuestados en Colombia, posicionando como el segundo país con mayor incidencia de este problema.

Estos datos reflejan, que los grupos terroristas han evolucionado para adaptarse a esta nueva era representando una mayor amenaza estatal en el anonimato, incitando la violencia, coordinando ataques, difundiendo discursos que afectan a la seguridad del Estado y sus ciudadanos, lo cual, demanda una respuesta eficaz ante las vulnerabilidades del ecosistema virtual.

En ese contexto, el terrorismo adopta expresiones propias de la criminalidad en red y se integra a lo que la doctrina ha denominado ciberterrorismo, entendido como la convergencia entre terrorismo y ciberespacio, donde permanecen los elementos constitutivos del terrorismo tradicional y lo que varía es el canal de ejecución.

Ahora bien, debido a la amplitud técnica y social de las TIC, resulta indispensable delimitar con precisión el fenómeno para evitar confusiones dogmáticas y expansiones punitivas innecesarias. Tomando como referencia la clasificación de los delitos en el ciberespacio —entre delitos ciber-dependientes y delitos ciber-habilitados— el ciberterrorismo presenta dos vertientes diferenciadas: terrorismo informático **y** terrorismo digital.

El terrorismo informático corresponde al uso directo de técnicas y herramientas digitales para atacar sistemas, redes o infraestructuras informáticas, produciendo daños técnicos; aquí la violencia se despliega sobre la tecnología misma como objeto de ataque.

En contraste, el Terrorismo Digital engloba delitos tradicionales potenciados por medios digitales: no persigue un daño técnico como fin, sino que instrumentaliza internet, plataformas y redes para difundir propaganda radical, reclutar, financiar, coordinar operaciones, manipular psicológicamente a la población o producir campañas masivas de intimidación y desinformación con finalidad terrorista

En esta modalidad, lo determinante es la apropiación simbólica y estratégica de la circulación de información para generar miedo y zozobra colectiva, sin necesidad de violencia física directa ni sabotaje técnico como núcleo del injusto.

En consecuencia, puede definirse el Terrorismo Digital como una derivación del ciberterrorismo por cuanto su forma de violencia tecnológica se encuentra en el plano comunicacional de las TIC: usando redes, plataformas y medios digitales.; en aras de difundir miedo, odio o desinformación, con el fin de afectar a la población civil o parte de ella, manipular la opinión pública y desestabilizar la estabilidad social o política

Considerando que, socava de manera silenciosa los propios pilares del orden democrático la confianza, y la seguridad digital derivada de la seguridad pública.

En efecto, el TDig se configura como una amenaza directa al bien jurídico de la seguridad digital, concebida como una manifestaciones la seguridad pública, en tanto busca salvaguardar a la población frente a actos dañinos para el pacto social , mediante el uso indebido de las TIC bajo el marco comunicacional digital (no físico, no técnico).

Bajo esta delimitación, el presente Proyecto de Ley se estructura exclusivamente sobre el Terrorismo Digital, el propósito de esta iniciativa no es duplicar tipos ni ampliar irreflexivamente el poder punitivo, sino cerrar la atipicidad del TDig mediante su reconocimiento como modalidad comisiva agravada del terrorismo tradicional, exclusivamente cuando el uso del medio digital incrementa el peligro contra la seguridad pública.

Por tanto, la conducta terrorista no cambia su estructura esencial: lo que se transforma es el canal. El medio digital maximiza el alcance del terror y acelera su capacidad de penetración social, pero el bien jurídico protegido permanece inalterado.

Hecha esta salvedad, el terrorismo previsto en el artículo 343 de la Ley 599 de 2000 protege la seguridad pública como bien jurídico colectivo. En el contexto contemporáneo, la llamada "seguridad digital" no constituye una categoría autónoma distinta, sino una manifestación funcional y actual de la seguridad pública en el ciberespacio; en consecuencia, la afectación terrorista digital debe entenderse como una forma de lesión a la misma seguridad pública, ahora expresada en un escenario tecnológico.

La unidad del bien jurídico impide justificar una tipificación independiente: no hay nuevo injusto penal, sino un modo de ejecución cualificado que incrementa el peligro concreto contra la seguridad pública.

Aunque el ordenamiento dispone de tipos sobre terrorismo (arts. 343 y ss.) y de delitos informáticos (Ley 1273 de 2009), no existe una previsión expresa que reconozca la modalidad digital del terrorismo como agravación específica. Esta ausencia genera dificultades de imputación integral frente a fenómenos como radicalización en línea, propaganda extremista, coordinación digital de violencia o campañas de intimidación masiva.

La respuesta estatal reciente ha operado principalmente desde la política pública preventiva de seguridad digital mediante CONPES 3995 de 2020 (Política Nacional de Seguridad Digital) y el CONPES 4144 de 2025 (Estrategia Nacional de Inteligencia Artificial), lo cual es necesario pero insuficiente cuando se está ante conductas con finalidad terrorista que comprometen gravemente el pacto social.

Sin embargo, el Proyecto se fundamenta en un modelo de Estado Social de Derecho, que limita el ius puniendi mediante legalidad estricta, proporcionalidad, culpabilidad y mínima intervención. Las transformaciones tecnológicas reclaman una adaptación razonable del derecho penal, pero no la creación de tipos abiertos, redundantes o simbólicos.

Además, que una expansión punitiva desmedida en clave de "amenaza digital" puede derivar en prácticas cercanas al Derecho Penal del Enemigo, donde el ciudadano es tratado como peligro potencial antes que como sujeto de derechos; por lo que este Proyecto evita esa deriva, preservando el derecho penal garantista y rechazando esquemas de excepción.

Atendiendo a lo anterior, la alternativa constitucionalmente adecuada es incorporar una circunstancia de agravación punitiva al terrorismo cuando se ejecute mediante medios digitales, sin alterar la estructura del tipo base.

ANTECEDENTES DE LA INICIATIVA.

A la fecha no existen antecedentes legislativos específicos orientados a regular de manera expresa el terrorismo cometido mediante medios digitales como modalidad comisiva del terrorismo tradicional. Si bien el ordenamiento penal colombiano contempla el delito de terrorismo (artículo 343 de la Ley 599 de 2000) y sus circunstancias de agravación (artículo 344), dichas disposiciones fueron concebidas bajo un contexto predominantemente físico y no incorporan de forma explícita el uso de medios digitales como factor de incremento del riesgo terrorista.

IMPACTO FISCAL

El presente Proyecto de Ley no crea nuevas entidades, no establece cargas administrativas adicionales permanentes ni implica ampliación estructural de planta de personal. Su

implementación se integra a las competencias ordinarias de la Fiscalía General de la Nación, la Policía Judicial y la Rama Judicial en materia de investigación y juzgamiento del terrorismo.

En consecuencia, no genera impacto fiscal directo adicional distinto al que pueda derivarse de procesos de capacitación y actualización técnica dentro de los presupuestos institucionales vigentes, en concordancia con las políticas públicas actuales de seguridad digital y fortalecimiento investigativo.