Cuestionario

Mayor (EJC) MANUEL RICARDO REY RIOS

Electiva - Habilidades Prácticas en el Ciberespacio

Escuela Superior de Guerra “General Rafael Reyes Prieto”
Bogotá D.C. Colombia
2025

Cuestionario

1. **¿Cuál es la diferencia fundamental, según el texto, entre "misinformation" y "disinformation"?**

La diferencia fundamental entre "misinformation" y "disinformation" radica en la intencionalidad.

La "disinformation" (desinformación) es información falsa generada deliberadamente con el fin de causar perjuicio. Por otro lado, la "misinformation" (información errónea) se refiere a información que, aun siendo falsa, se distribuye sin una intención deliberada de causar daño, sino que el emisor la emite presumiendo su veracidad. El texto también menciona el término "malinformation", que es información verdadera distribuida de manera sesgada o fuera de contexto con un propósito malicioso.

2. **Según el Reuters Institute Digital News Report 2023, ¿qué tendencia preocupante se observa en España con respecto al interés por las noticias?**

Según el Reuters Institute Digital News Report 2023, la tendencia preocupante en España es una de las mayores bajadas en el interés por las noticias en comparación con otros países.

El interés pasó de un 85% de personas que indicaban tener un interés alto o muy alto por las noticias en 2015 al 51% en 2023, lo que representa una disminución de 34 puntos porcentuales. Además, la desconfianza de los lectores en los medios de comunicación alcanzó un récord del 40% en estos nueve años de encuesta, sobre todo entre los menores de 45 años. Esta situación crea una "tormenta perfecta" donde la desinformación ha hecho acto de presencia de forma masiva a partir de las redes sociales.

3. **¿Cómo se comparan, según los experimentos de Vosoughi, Roy y Aral (2018), la velocidad y facilidad de difusión de noticias falsas frente a las verdaderas?**

Según los experimentos de Vosoughi, Roy y Aral (2018), las noticias falsas se difunden más fácilmente y más rápido que las verdaderas.

En dicho estudio, los autores concluyen que el 1% de las noticias falsas que más se difundieron llegaron a entre 1.000 y 100.000 personas, mientras que el 1% de las verdaderas que más se difundieron rara vez llegaron a más de 1.000 personas. Estos patrones de difusión tan diferentes permiten utilizar las trazas que deja la información al propagarse por las redes para diferenciar la información verídica de la información falsa.

4. **¿Qué ventaja clave ofrecen las redes latentes de difusión sobre los modelos epidemiológicos para el estudio de la desinformación?**

La ventaja clave que ofrecen las redes latentes de difusión sobre los modelos epidemiológicos es que no solo permiten predecir cómo evolucionará la propagación de piezas de información, sino que también permiten **conocer quién la propaga y cómo lo hace**. A diferencia de los modelos epidemiológicos que son anónimos y no permiten saber qué personas están en cada grupo ni por qué están en él, las redes latentes de difusión permiten identificar la estructura de las relaciones dentro de la red, los actores más influyentes (como "controladores del discurso" o "influencers"), las comunidades y la densidad de conexiones.

5. **¿Qué son los "grandes modelos de lenguaje" y cuál es su principal riesgo en el contexto de la desinformación?**

Los "grandes modelos de lenguaje" (large language models en inglés) son sistemas de inteligencia artificial que, gracias a la arquitectura Transformer, han otorgado una capacidad sin precedentes para generar texto de calidad de manera controlada y a velocidades altísimas. Su principal riesgo en el contexto de la desinformación radica en que bajan significativamente los requisitos necesarios para generar contenido de una calidad aceptable, permitiendo la creación de artículos con información falsa en tiempo récord. Estos modelos no tienen noción sobre si el resultado que producen es veraz y pueden ser engañados para generar información falsa, incluso después de haber puesto objeciones. Esto los convierte en la herramienta perfecta para llevar a cabo campañas de desinformación invirtiendo pocos recursos.

6. **¿Cómo facilita la accesibilidad de los modelos de IA la generación de desinformación?**

La accesibilidad de los modelos de IA facilita la generación de desinformación al reducir la barrera de entrada de manera significativa. En cuestión de semanas, se ha pasado de necesitar equipos profesionales de alto rendimiento y amplios conocimientos de informática para ejecutar dichos sistemas a poderlo hacer en equipos portátiles domésticos con un conocimiento mínimo. Esta accesibilidad masiva, aunque positiva para el avance científico, tiene un lado negativo, ya que reduce el costo de generar información engañosa y, por ende, el costo de realizar campañas de desinformación. Además, los modelos generativos más pequeños, aunque menos potentes, pueden generar microtextos aptos para redes sociales, y la combinación con la economía de microencargos ("gig economy") ha hecho que realizar campañas de manipulación sea más sencillo que nunca.

7. **¿Qué son las "cajas negras" en el contexto de la IA explicativa y cuál es el desafío asociado?**

En el contexto de la IA explicativa, las "cajas negras" son modelos de IA muy complejos, como los basados en redes neuronales profundas, bajo los que operan millones de parámetros numéricos y de los cuales resulta imposible obtener conclusiones y explicaciones comprensibles. El desafío asociado es avanzar hacia otro tipo de modelos u obtener explicaciones de estas "cajas negras", un proceso que "llevará tiempo, ya que conlleva solucionar importantes desafíos". Esta opacidad dificulta la comprensión de por qué un sistema toma una decisión concreta, lo cual es imprescindible para confiar en la IA.

8. **¿Qué implicaciones tiene el concepto de "Inteligencia Artificial General (AGI)" para la lucha contra la desinformación?**

El concepto de "Inteligencia Artificial General (AGI)", definida como una IA capaz de pensar, aprender y actuar como lo haría un humano, tiene implicaciones ambivalentes para la lucha contra la desinformación. Aunque puede mejorar la capacidad de verificación de información, dado que los grandes modelos de lenguaje solo pueden seguir mejorando, su mejora inevitablemente supondrá la obtención de capacidades superiores para generar y apoyar la desinformación. El texto señala que un buen modelo de lenguaje será capaz de generar desinformación cada vez más engañosa. Por desgracia, el desinformador siempre tiene ventaja en este intercambio, pues es el primero en actuar antes de ser verificado.

9. **¿Qué normativas europeas importantes se mencionan en relación con la IA y la privacidad?**

Las normativas europeas importantes mencionadas en relación con la IA y la privacidad son: el **Reglamento General de Protección de Datos (RGPD)**, aprobado el 27 de abril de 2016, que establece el derecho a la protección de datos personales y los principios que deben regir su tratamiento; y el **Libro Blanco de la IA**, enmarcado en la Estrategia Digital de la Unión Europea, que fija las bases para el desarrollo de la IA con especial atención a las implicaciones en los datos personales. También se menciona que la **Ley de Inteligencia Artificial** está cada vez más cerca.

10. **¿Cómo garantiza FacTeR-Check el cumplimiento de la normativa de protección de datos al analizar redes sociales?**

FacTeR-Check garantiza el cumplimiento de la normativa de protección de datos al analizar redes sociales prestando especial atención a las fuentes de datos que utiliza. Para ello, es imprescindible que se verifique previamente que, por ejemplo, los tuits analizados son de usuarios con perfiles públicos o, si son privados, que han dado su consentimiento para su uso con esta finalidad, tal como establece la normativa de protección de datos. Además, la

herramienta se diseña desde el inicio observando los principios de protección de datos y privacidad, y teniendo en cuenta principios de la IA como la explicabilidad, la seguridad o la supervisión humana.

11. Analice las diferentes formas en que la Inteligencia Artificial puede ser utilizada tanto para generar como para combatir la desinformación, basándose en los ejemplos y conceptos presentados en el texto.

La Inteligencia Artificial (IA) se ha convertido en una herramienta de doble filo en el ecosistema de la información, con capacidades avanzadas tanto para generar como para combatir la desinformación.

Uso de la IA para Generar Desinformación:

- **Generación de Texto y Bots:** Los "grandes modelos de lenguaje" (LLMs) como ChatGPT, basados en la arquitectura Transformer, han revolucionado la capacidad de generar texto de alta calidad, convincente y a velocidades altísimas. Un actor malicioso puede pedir a estos modelos que escriban noticias basadas en información incorrecta con intencionalidad dañina, obteniendo artículos falaces en minutos. Los modelos no comprenden la veracidad, pueden ser engañados para generar contenido inapropiado o falso, y su accesibilidad masiva reduce el costo de campañas de desinformación. Además, estos modelos permiten la creación de bots sofisticados que simulan comportamiento humano y publican mensajes maliciosos de forma regular, útiles para la propaganda política.

- **Manipulación del Medio Visual (Imágenes y Vídeos):** La IA permite la creación de "deep fakes" mediante redes neuronales profundas para generar caras de personas que no existen, intercambiar rostros o alterar expresiones faciales, lo que es peligroso para suplantar a figuras políticas. La técnica de "image inpainting" puede eliminar personas u objetos sensibles de fotos, o generar nuevos objetos usando texto. Estas aplicaciones facilitan la introducción de simbología ideológica, el reemplazo de contextos engañosos o la sustitución de objetos controvertidos. Aunque más compleja, la manipulación de vídeos también ha avanzado para alterar expresiones en un formato animado.

- **Manipulación de Audio:** Es una modalidad menos explorada pero con aplicaciones en desinformación. Incluye la clonación de voz (imitando tono, ritmo y timbre de figuras públicas con pocas muestras de audio) , la manipulación de voz para alterar ligeramente mensajes y la sintetización de voz para generar audios que se hagan pasar por figuras de autoridad anónimas o interacciones entre agentes de síntesis. La

sinergia con la generación de texto permite crear discursos completos y automáticos con la voz deseada en tiempo real.

Uso de la IA para Combatir la Desinformación:

- **Herramientas de Detección y Verificación (FacTeR-Check):** El proyecto CIVIC desarrolló FacTeR-Check, una herramienta que utiliza técnicas avanzadas de procesamiento del lenguaje natural (NLP) basadas en la arquitectura Transformer para verificar frases o afirmaciones. Su enfoque semiautomático contrasta textos con una base de datos de hechos ya verificados por entidades de "fact-checking", garantizando alta fiabilidad y actualidad. Esto se logra mediante módulos de similitud semántica (que filtran hechos relevantes) y de inferencia del lenguaje natural (que analiza la relación de implicación, contradicción o neutralidad entre la frase a verificar y los hechos candidatos).

- **Monitorización en Redes Sociales:** FacTeR-Check integra funcionalidades para analizar la desinformación en redes sociales como Twitter. Permite recopilar tuits relevantes usando palabras clave y entidades nombradas extraídas por modelos como KeyBERT y NER. Luego, filtra semánticamente los tuits y usa la inferencia del lenguaje natural para etiquetarlos como "implicación", "contradicción" o "neutral" respecto al bulo. Esto ayuda a entender las dinámicas de propagación, identificar usuarios influyentes y observar la lucha entre la desinformación y sus desmentidos.

- **Multilingüismo y Adaptabilidad:** FacTeR-Check ofrece un enfoque multilingüe completo, permitiendo contrastar y analizar información en cualquier idioma, lo que diluye las barreras lingüísticas en la lucha global contra la desinformación.

- **Detección Forense:** Para las manipulaciones visuales y de audio, la IA permite detectar ciertos rastros o marcas que estas manipulaciones dejan en el contenido, mediante análisis forenses y técnicas de deep learning.

En conclusión, la IA ha proporcionado un abanico de herramientas sin precedentes que permiten generar contenido multimedia de apariencia muy realista, haciendo verdaderamente complicado distinguir el contenido real del generado. La única manera de luchar contra esta desinformación es precisamente haciendo uso de los últimos avances de inteligencia artificial, tomando una posición de ventaja.

12. **Discuta el papel de la Inteligencia Artificial Explicativa (XAI) en la mejora de la confianza pública en los sistemas de detección de desinformación y en la educación de los usuarios. ¿Cuáles son los principales obstáculos para su desarrollo?**

La Inteligencia Artificial Explicativa (XAI) es fundamental para mejorar la confianza pública en los sistemas de detección de desinformación y en la educación de los usuarios, al hacer los sistemas más comprensibles y transparentes.

Papel de la XAI:

- **Mejora de la Confianza y Transparencia:** Para que se pueda confiar en la IA, es imprescindible que ofrezca razones y argumentos concretos que permitan conocer por qué un sistema toma una decisión específica. Los avances en la IA explicable permitirán a los usuarios una mejor comprensión de cómo y por qué se clasifica el contenido como desinformación, adquiriendo simultáneamente mayor confianza en estas tecnologías. Además, una mayor transparencia facilitará el descubrimiento y la corrección de posibles sesgos o errores en el sistema.

- **Descomposición y Contextualización de la Desinformación:** La IA explicativa permitirá descomponer la desinformación de manera más efectiva, determinando piezas de texto contrastables y ayudando a los usuarios a entender por qué ciertas afirmaciones son incorrectas. A medida que estos sistemas avancen, podrán proporcionar el contexto necesario para entender la desinformación.

- **Personalización y Educación del Usuario:** Se espera que la XAI mejore su capacidad de personalizar el grado de detalle y el tipo de explicación en función de las necesidades del usuario. Es de esperar que la IA explicativa no solo ayude a detectar la desinformación, sino que también tenga un papel importante en la educación de los usuarios, permitiéndoles aprender a reconocer la desinformación por sí mismos al proporcionarles una visión detallada de cómo se detecta.

- **Apoyo a Expertos:** Los expertos o científicos de diversas áreas también podrán entender mejor sus propios modelos y sus datos, lo que puede llevar a mejoras en su precisión y efectividad.

Principales Obstáculos para su Desarrollo:

- **Modelos de "Caja Negra":** El principal obstáculo es que la mayoría de los modelos actuales que consiguen excelentes resultados se basan en "cajas negras". Estos

modelos son muy complejos, operan con millones de parámetros numéricos y de ellos resulta imposible obtener conclusiones y explicaciones claras.

- **Desafío Técnico y Temporal:** Avanzar hacia otro tipo de modelos o lograr obtener explicaciones de estas "cajas negras" es un proceso que "llevará tiempo, ya que conlleva solucionar importantes desafíos". Esto implica una complejidad inherente a la arquitectura de muchos de los modelos de IA más potentes hoy en día.

En síntesis, la XAI es una promesa para construir confianza y empoderar a los usuarios y expertos en la lucha contra la desinformación, pero su plena realización está condicionada a la superación de los retos técnicos derivados de la opacidad de los modelos de IA actuales.

13. **Compare los modelos epidemiológicos y las redes latentes de difusión como enfoques para estudiar la propagación de la desinformación en las redes sociales. ¿Qué información específica puede obtenerse de cada tipo de modelo?**

Para comprender la propagación de la desinformación en redes sociales, el texto presenta los modelos epidemiológicos y las redes latentes de difusión como dos enfoques distintos, cada uno con sus propias características y la capacidad de ofrecer información específica.

Modelos Epidemiológicos:

- **Concepto y Analogía:** Estos modelos matemáticos simulan un proceso de difusión inspirándose en los brotes epidémicos, estableciendo una analogía entre la propagación de la información y la de un virus. La población se divide en grupos (como "susceptibles", "infectadas" y "recuperadas" en el modelo SIR) y se definen probabilidades para pasar de un grupo a otro. Se ajustan a partir de secuencias de activación, que registran el momento en que un usuario ha hablado de una pieza de información, sin conocer las interacciones directas entre usuarios.
- **Información Específica que se Obtiene:**
    - Permiten predecir cuántas personas habrá en cada uno de los grupos en un momento dado.
    - Hacen posible realizar simulaciones de qué pasaría si se cambian los parámetros de difusión.
    - Son útiles para detectar que hay un flujo anómalo de información.

- **Limitación Clave:** Son modelos **anónimos**. No son capaces de saber qué personas están en cada grupo ni por qué están en él. Por lo tanto, es imposible saber quiénes

son los agentes encargados de difundir una pieza de información y, consecuentemente, cómo actuar ante ellos.

Redes Latentes de Difusión:

- **Concepto y Funcionamiento:** Son un modelo generativo de redes sociales que permite modelizar la difusión de información entre los individuos de una red a lo largo del tiempo. A diferencia de los modelos epidemiológicos, no son anónimos. Se ajustan a partir de datos empíricos, transformando las secuencias de activación en "cascadas de activación", que sí tienen en cuenta la interacción entre usuarios. Esto permite calcular la influencia que tiene cada nodo en otros nodos, es decir, la dirección y el tamaño de las flechas de influencia.
- **Información Específica que se Obtiene:**
    - Permiten conocer **quién propaga la información y cómo lo hace**.
    - Permiten identificar la estructura de las relaciones dentro de la red, los actores más influyentes, las comunidades y la densidad de conexiones. Por ejemplo, se pueden diferenciar usuarios "controladores del discurso", "influencers" (como el usuario azul en la Figura 1.4) y "receptores" (usuarios grises en la Figura 1.4).
    - Facilitan estudios estadísticos para buscar patrones de influencia entre usuarios.
- **Limitación Clave:** Ajustar un modelo de red de difusión con una precisión razonable es complicado debido a la gran cantidad de datos que requiere. Dado que eliminan el componente anónimo, se requiere disponer de suficiente información sobre todas y cada una de las cuentas incluidas en la red bajo estudio, lo cual puede ser difícil de conseguir debido a la naturaleza de las redes sociales donde las cuentas se crean y eliminan con frecuencia.

En conclusión, mientras los modelos epidemiológicos proporcionan una visión agregada y predictiva de la propagación de la desinformación a nivel de población, las redes latentes de difusión ofrecen una comprensión granular al identificar a los actores específicos, sus roles de influencia y las interacciones mutuas, lo que es esencial para actuar de manera dirigida contra la desinformación.

14. Examine la relación entre la accesibilidad de las herramientas de IA generativa y el aumento potencial de la desinformación. ¿Qué estrategias se sugieren para mitigar este riesgo?

La relación entre la accesibilidad de las herramientas de IA generativa y el aumento potencial de la desinformación es directa y alarmante. El texto destaca cómo los recientes avances han

"bajado la barrera de entrada de manera significativa" , permitiendo a un público masivo generar contenido que antes requería conocimientos técnicos y recursos especializados. Esta facilidad reduce el costo de generar información engañosa, lo que a su vez disminuye el costo de realizar campañas de desinformación. La combinación con la "economía de microencargos" o "gig economy" hace que las campañas de manipulación en redes sociales sean "más sencillo que nunca". Se espera que esta tendencia lleve a un "boom de desinformación generada (o asistida) por IA" cuando los modelos sean lo suficientemente accesibles y sus resultados engañosos como para pasar por reales.

Estrategias Sugeridas para Mitigar este Riesgo: El texto propone un enfoque multifacético para mitigar este riesgo, que incluye:

- **Desarrollo de Nuevos Modelos de Clasificación:** Afortunadamente, con los nuevos modelos de generación también aparecen nuevos modelos de clasificación utilizables para su detección. La herramienta FacTeR-Check es un ejemplo de cómo se puede anticipar la plasticidad de la desinformación utilizando una base de datos de conocimiento experto para la verificación automática.
- **Explotación de Múltiples Características de la Información:** Las técnicas para detener la desinformación deben ir más allá del contenido y las fuentes, explorando también el **estilo** y el **contexto** de las informaciones. Por ejemplo, analizar si un texto está escrito en un estilo parecido al de otra desinformación o si la red de contactos del autor propaga frecuentemente desinformación.
- **Desarrollo de Técnicas "a priori" y "a posteriori":** Es necesario distinguir y desarrollar técnicas que evalúen el contenido *a posteriori* (como FacTeR-Check, que utiliza fuentes de conocimiento verificadas) y técnicas *a priori* que evalúen la fiabilidad del contenido sin verificarlo con fuentes, observando el estilo y el contexto. Aunque el verificador siempre actúa con desventaja temporal, se debe buscar explotar todas las vías posibles para ralentizar y detener la generación maliciosa.
- **Fomento de la IA Explicativa (XAI):** La IA explicativa es fundamental para la lucha contra la desinformación, ya que hará los sistemas más comprensibles y transparentes, aumentando la confianza de los usuarios y educándolos para reconocer la desinformación.
- **Alfabetización Mediática:** Es "imprescindible una sólida educación en alfabetización mediática".
- **Regulación Efectiva de Plataformas:** Se menciona la importancia de la "regulación efectiva de las plataformas de redes sociales para combatir la difusión de información falsa".

- **Colaboración e Investigación Continua:** El informe enfatiza que combatir este problema requiere un enfoque "multifacético y multidisciplinar" y que no será posible sin un gran número de investigadores y empresas que se apoyen y colaboren para inclinar la balanza hacia un uso benigno de la tecnología.

En definitiva, la accesibilidad de la IA generativa amplifica exponencialmente el riesgo de desinformación. La mitigación de este riesgo requiere una combinación de avances tecnológicos en detección (incluyendo XAI), estrategias de análisis multifactoriales, educación ciudadana y un marco regulatorio robusto que fomente el uso responsable de la IA.

15. Analice las consideraciones éticas y de privacidad asociadas con el uso de la Inteligencia Artificial para combatir la desinformación, haciendo referencia a las normativas europeas mencionadas e identificado si existen normativas similares en nuestro país.

El uso de la Inteligencia Artificial para combatir la desinformación, si bien necesario y prometedor, conlleva importantes consideraciones éticas y de privacidad que la Unión Europea ha abordado activamente.

a) Consideraciones Éticas y de Privacidad Asociadas:

- **Protección de Datos Personales:** La IA incide de forma evidente en la privacidad de las personas. Es fundamental que cualquier sistema diseñado para combatir la desinformación sea respetuoso con los principios de protección de datos y privacidad. Esto implica que las herramientas deben diseñarse desde el inicio observando estos principios ("privacy-by-design").
- **Acceso a Datos y Consentimiento:** La fuente de datos es crucial. Para cumplir con la normativa, herramientas como FacTeR-Check deben verificar que los datos, por ejemplo, tuits, provengan de usuarios con perfiles públicos o que, si son privados, se haya obtenido su consentimiento expreso para el uso con esta finalidad.
- **Otros Derechos Fundamentales:** La preocupación por el crecimiento de la IA no solo afecta a la privacidad, sino también a otros derechos fundamentales como la libertad de expresión, la libertad de pensamiento o la no discriminación. La toma de decisiones basada en el tratamiento de datos debe respetar estos derechos.
- **Transparencia y Explicabilidad (XAI):** La explicabilidad es un principio clave para la IA. Los sistemas de IA, especialmente cuando afectan a las personas y sus derechos, deben cumplir con los requisitos de transparencia y explicabilidad. Esto permite a los usuarios comprender cómo y por qué se clasifica el contenido como desinformación y, a su vez, descubrir y corregir posibles sesgos o errores.

b) Normativas Europeas Mencionadas: La Unión Europea ha implementado diversas iniciativas para proteger la privacidad en el contexto del desarrollo de la IA:

- **Reglamento General de Protección de Datos (RGPD) (UE) 2016/679:** Aprobado el 27 de abril de 2016, este reglamento fundamental recuerda que "toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan". Desarrolla los principios que deben regir el tratamiento de datos personales, los derechos del interesado y las obligaciones de los responsables.
- **Libro Blanco de la IA (2020):** Este documento se enmarca en la Estrategia Digital de la Unión Europea y establece el marco general para el desarrollo de la IA en el ámbito europeo, con especial atención a las implicaciones en los datos personales.
- **Ley de Inteligencia Artificial (AI Act):** Se menciona que esta ley está más cerca y aborda preocupaciones no solo sobre la privacidad, sino también sobre la protección de otros derechos fundamentales como la libertad de expresión, el pensamiento y la no discriminación.

c) Normativas Similares en Colombia (considerando el contexto del usuario):

En Colombia, aunque no existe una ley específica que regule integralmente el uso de la Inteligencia Artificial como en Europa, sí hay un marco normativo y estratégico en evolución:

- **Ley 1581 de 2012 (Ley de Protección de Datos Personales):** Esta es la principal normativa en Colombia en materia de protección de datos personales. Establece el régimen general aplicable al tratamiento de datos, incluyendo principios como la legalidad, finalidad, libertad, veracidad, transparencia, acceso y circulación restringida, seguridad y confidencialidad. Otorga derechos a los titulares de la información (acceso, rectificación, supresión de datos) y establece obligaciones para los responsables y encargados del tratamiento de datos personales. La Superintendencia de Industria y Comercio (SIC) es la entidad encargada de velar por su cumplimiento.
- **Documento CONPES 4144 de 2023 - Política Nacional para el Desarrollo y la Adopción de la Inteligencia Artificial:** Este documento reciente del Estado colombiano (febrero de 2023) establece una hoja de ruta para promover el desarrollo y la adopción de la IA de manera ética, responsable e inclusiva. Incluye principios éticos para el desarrollo y uso de la IA, como la transparencia, la explicabilidad, la equidad, la privacidad y la no discriminación, y busca la coherencia con la Ley 1581 de 2012 y estándares internacionales como el RGPD europeo. Aunque un CONPES no tiene fuerza de ley, es una política pública que orienta las acciones del gobierno en la materia.
- **Iniciativas Legislativas:** Ha habido y continúan existiendo proyectos de ley en el Congreso colombiano que buscan regular la IA en aspectos como la responsabilidad, los sesgos algorítmicos y la transparencia, aunque aún no se ha materializado una ley específica de IA aprobada y en vigor.

En conclusión, el desarrollo y uso de la IA para combatir la desinformación requiere un equilibrio delicado entre la eficacia tecnológica y el respeto por los derechos fundamentales. La Unión Europea ha establecido un marco robusto con el RGPD y el Libro Blanco de la IA, avanzando hacia una ley de IA. En Colombia, la Ley 1581 de 2012 es el pilar de la protección de datos, y el reciente CONPES 4144 de 2023 sienta las bases para un desarrollo ético y responsable de la IA, aunque el marco regulatorio específico para la IA sigue en evolución. La adopción de buenas prácticas europeas, como el "privacy-by-design", es esencial para garantizar una implementación ética y efectiva en el contexto colombiano.