Escuela Superior de Guerra “General Rafael Reyes Prieto”

Cuestionario de Desinformación

My. Edna Giannine Robles Ocampo

Habilidades Prácticas en el Ciberespacio

Jaider Ospina Navas

Curso de Estado Mayor 2025

01 de julio de 2025

Cuestionario de Desinformación

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

Según el documento Luchando contra la desinformación mediante la inteligencia artificial, la diferencia fundamental entre “misinformation” y “disinformation” radica en la intencionalidad con la que se difunde la información. El término misinformation se refiere a información errónea o falsa que se distribuye sin intención deliberada de causar daño, ya que el emisor la comparte creyendo que es cierta. En contraste, disinformation hace referencia a información falsa generada y difundida de manera deliberada con el propósito de provocar perjuicio en la audiencia o manipularla de forma maliciosa (Martín García et al., 2024, p. 15).

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 documento Luchando contra la desinformación mediante la inteligencia artificial, el Reuters Institute Digital News Report 2023 destaca una tendencia preocupante en España: el interés por las noticias ha caído drásticamente en los últimos años. Específicamente, se ha pasado del 85 % de personas que declaraban tener un interés alto o muy alto en las noticias en 2015, al 51 % en 2023, lo que supone una disminución de 34 puntos porcentuales. Esta pérdida de interés es una de las mayores entre los países analizados y, junto con el aumento de la desconfianza en los medios, configura un “caldo de cultivo” ideal para la propagación de la desinformación (Martín García et al., 2024, p. 13).

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?**

De acuerdo con el documento Luchando contra la desinformación mediante la inteligencia artificial, los experimentos de Vosoughi, Roy y Aral (2018) demostraron que las noticias falsas se difunden con mayor facilidad y rapidez que las verdaderas. El estudio citado concluye que el 1 % de las noticias falsas más compartidas alcanzaron entre 1.000 y 100.000 personas, mientras que el 1 % de las noticias verdaderas más difundidas rara vez superó las 1.000 personas. Esta diferencia sustancial en los patrones de propagación sirve como base

para desarrollar métodos de detección temprana de desinformación, aprovechando la mayor viralidad de las noticias falsas (Martín García et al., 2024, p. 21).

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

El documento Luchando contra la desinformación mediante la inteligencia artificial explica que la ventaja clave de las redes latentes de difusión sobre los modelos epidemiológicos radica en su capacidad para identificar quién propaga la desinformación y cómo lo hace. Mientras que los modelos epidemiológicos son anónimos y solo permiten detectar la existencia de un flujo anómalo de información (sin saber quién lo causa), las redes latentes de difusión eliminan el componente anónimo, permitiendo modelar explícitamente las interacciones entre usuarios. Esto posibilita conocer la dirección e intensidad de la influencia entre cuentas, identificar a los actores más influyentes y entender la estructura de la propagación en la red, lo cual es esencial para diseñar estrategias de intervención más efectivas contra la desinformación (Martín García et al., 2024, p. 24).

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

El documento Luchando contra la desinformación mediante la inteligencia artificial describe a los grandes modelos de lenguaje (en inglés, large language models) como sistemas de inteligencia artificial basados en la arquitectura Transformer, capaces de generar texto de alta calidad de forma controlada y a gran velocidad. Estos modelos, como GPT, permiten crear contenido textual realista y convincente con muy poco esfuerzo técnico. Su principal riesgo en el contexto de la desinformación radica en que reducen drásticamente las barreras para producir artículos falsos, bulos y narrativas engañosas de apariencia creíble. Al facilitar la generación masiva y rápida de texto engañoso, contribuyen significativamente a la propagación de la desinformación, ya que incluso personas sin habilidades avanzadas pueden crear contenido persuasivo y difundirlo ampliamente (Martín García et al., 2024, p. 28).

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

El documento Luchando contra la desinformación mediante la inteligencia artificial señala que la creciente accesibilidad de los modelos de IA ha facilitado notablemente la generación de desinformación. Gracias al desarrollo de modelos de código abierto y a su disponibilidad en repositorios públicos, hoy en día cualquier persona con un ordenador doméstico de alta gama y conocimientos básicos puede ejecutar estas herramientas. Antes, se necesitaban equipos profesionales y experiencia avanzada. Esta democratización de la tecnología ha reducido drásticamente el costo y la barrera de entrada para crear contenido engañoso. Así, la facilidad de acceso masivo permite que actores maliciosos generen de forma sencilla y económica textos, imágenes o audios falsos con apariencia realista, habilitando campañas de desinformación más baratas, veloces y difíciles de controlar (Martín García et al., 2024, p. 27).

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

En el documento Luchando contra la desinformación mediante la inteligencia artificial, se explica que en el contexto de la IA explicativa, el término “cajas negras” se refiere a modelos de inteligencia artificial cuyos procesos internos son opacos o difíciles de interpretar para los humanos. Aunque estos modelos pueden ofrecer resultados muy precisos, el problema es que no se puede entender ni justificar fácilmente cómo llegaron a sus conclusiones. El desafío asociado radica en la necesidad de desarrollar sistemas de IA que no solo sean efectivos en detectar o combatir la desinformación, sino que además puedan explicar sus decisiones de forma comprensible. Esto es fundamental para generar confianza en sus resultados y permitir que usuarios y expertos validen, supervisen y mejoren los sistemas de IA, evitando así errores, sesgos o manipulaciones inadvertidas (Martín García et al., 2024, p. 48).

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

Según el documento Luchando contra la desinformación mediante la inteligencia artificial, el concepto de Inteligencia Artificial General (AGI) implica el desarrollo de sistemas de IA capaces de realizar cualquier tarea cognitiva humana con un nivel de competencia similar o superior al nuestro. En el contexto de la lucha contra la desinformación, la AGI presenta implicaciones tanto prometedoras como preocupantes. Por un lado, podría ofrecer herramientas extraordinariamente potentes para detectar, analizar y contrarrestar la desinformación de forma automatizada y precisa, superando las limitaciones actuales. Por otro lado, también supone un riesgo considerable, ya que actores maliciosos podrían emplearla para generar y difundir campañas de desinformación mucho más sofisticadas, persuasivas y difíciles de detectar. Por ello, el documento enfatiza que es crucial considerar desde ahora los desafíos éticos, técnicos y de gobernanza que plantea el desarrollo de la AGI para mitigar sus posibles usos maliciosos (Martín García et al., 2024, p. 49).

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

En el documento Luchando contra la desinformación mediante la inteligencia artificial, se mencionan dos normativas europeas clave relacionadas con la IA y la privacidad. La primera es el Reglamento General de Protección de Datos (GDPR), que establece requisitos estrictos sobre la recopilación, el almacenamiento y el tratamiento de datos personales para proteger la privacidad de los ciudadanos europeos. La segunda es la propuesta de la Ley de Inteligencia Artificial de la Unión Europea (EU AI Act), que busca regular el desarrollo y uso de sistemas de IA en función de su nivel de riesgo, imponiendo mayores controles y obligaciones para aplicaciones de alto riesgo. El documento destaca que estas normativas son esenciales para garantizar que el avance de la IA se haga de forma ética, segura y respetuosa con los derechos fundamentales, incluyendo la protección frente a usos abusivos que puedan vulnerar la privacidad o facilitar la desinformación (Martín García et al., 2024, p. 49).

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

El documento Luchando contra la desinformación mediante la inteligencia artificial explica que la herramienta FacTeR-Check fue diseñada para cumplir con la normativa de protección de datos, especialmente el Reglamento General de Protección de Datos (GDPR) de la UE, al analizar la desinformación en redes sociales. Para ello, se asegura de analizar exclusivamente información pública disponible en estas plataformas, sin procesar datos privados ni realizar identificación personal no consentida de los usuarios. Además, el enfoque de FacTeR-Check se basa en estudiar patrones agregados de difusión y características semánticas del contenido, evitando la recolección o el tratamiento de información sensible o privada. De este modo, la herramienta permite detectar y contrarrestar la desinformación respetando la legalidad y los derechos fundamentales de privacidad de las personas (Martín García et al., 2024, p. 49).

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.

El documento Luchando contra la desinformación mediante la inteligencia artificial ofrece un análisis detallado y equilibrado sobre cómo la Inteligencia Artificial (IA) puede desempeñar un doble papel en el fenómeno de la desinformación: como herramienta para generarla y también para combatirla.

En cuanto a su uso para generar desinformación, el texto destaca el papel de los grandes modelos de lenguaje (LLM) que permiten crear textos falsos de alta calidad de forma rápida y barata. Estos modelos, basados en arquitecturas como Transformer, pueden ser manipulados para escribir artículos, titulares o argumentos convincentes, incluso sobre temas sensibles como la salud pública o el cambio climático, reduciendo drásticamente la barrera técnica para producir bulos (Martín García et al., 2024, p. 28). Además, la IA generativa se aplica a la creación de imágenes y vídeos ultrarrealistas (deepfakes) y audios manipulados, amplificando la capacidad de engaño y haciendo que las falsedades sean más creíbles (Martín García et al., 2024, p. 31–35). Estas herramientas también se han democratizado gracias al

código abierto y a plataformas accesibles que permiten a casi cualquier persona producir contenidos engañosos con pocos recursos (Martín García et al., 2024, p. 27).

Por otro lado, la IA también se está empleando para combatir la desinformación mediante sistemas automatizados de detección y verificación. Ejemplos concretos incluyen el uso de análisis de similitud semántica para comparar contenidos sospechosos con fuentes verificadas, y modelos de inferencia de lenguaje natural para evaluar la veracidad de afirmaciones (Martín García et al., 2024,p. 38). Herramientas como FacTeR-Check, desarrollada en el Proyecto CIVIC, integran estas técnicas para monitorear redes sociales, identificar patrones anómalos de difusión y detectar campañas de desinformación (Martín García et al., 2024, p. 40–44). Además, se aplican modelos de redes latentes de difusión para mapear la propagación de información en redes sociales, permitiendo identificar actores influyentes y dinámicas de manipulación (Martín García et al., 2024, p. 24).

En síntesis, el texto subraya que la IA es una espada de doble filo: mientras ofrece medios extraordinariamente eficaces para crear y diseminar desinformación a gran escala, también brinda herramientas poderosas para detectar, analizar y frenar estos mismos fenómenos. Por ello, se enfatiza la necesidad de desarrollar IA explicativa, capaz de justificar sus decisiones, y de regular su uso de manera responsable para maximizar sus beneficios y minimizar sus riesgos (Martín García et al., 2024, p. 48–49).

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?

El documento Luchando contra la desinformación mediante la inteligencia artificial subraya que la Inteligencia Artificial Explicativa (XAI) desempeña un papel esencial en la mejora de la confianza pública en los sistemas de detección de desinformación y en la educación de los usuarios. La razón fundamental es que, a diferencia de las llamadas “cajas negras” modelos opacos cuyos procesos internos son difíciles de interpretar, la IA explicativa busca ofrecer justificaciones comprensibles y transparentes sobre cómo llega a sus conclusiones (Martín García et al., 2024, p. 48).

En el contexto de la lucha contra la desinformación, la XAI permite que periodistas, verificadores, reguladores y ciudadanos entiendan por qué un sistema considera que una

afirmación es falsa o identifica un patrón anómalo de difusión. Esta capacidad de explicación no solo fortalece la confianza en las herramientas de detección reduciendo sospechas de censura o arbitrariedad, sino que también educa a los usuarios al mostrarles de manera comprensible los mecanismos de manipulación o las características de un bulo. Así, la XAI puede contribuir a una alfabetización mediática más robusta, ayudando a las personas a reconocer mejor la desinformación incluso fuera del ámbito de las plataformas automatizadas (Martín García et al., 2024, p. 48).

No obstante, el documento advierte que el desarrollo de IA explicativa enfrenta importantes obstáculos. Uno de los principales desafíos técnicos es lograr un equilibrio entre la precisión del modelo y su interpretabilidad, ya que los modelos más complejos y precisos suelen ser también los más opacos. Además, existe el problema de cómo diseñar explicaciones que sean comprensibles y útiles para distintos perfiles de usuarios, desde técnicos hasta el público general. Finalmente, la IA explicativa debe también evitar revelar información sensible o permitir ataques adversariales derivados de una excesiva transparencia en sus mecanismos internos. Todo esto convierte el desarrollo de la XAI en un reto multidisciplinar que combina aspectos técnicos, éticos, comunicativos y legales (Martín García et al., 2024, p. 48).

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?

El documento Luchando contra la desinformación mediante la inteligencia artificial describe en detalle dos enfoques principales para estudiar la propagación de la desinformación en redes sociales: los modelos epidemiológicos y las redes latentes de difusión.

Los modelos epidemiológicos se inspiran en el análisis de la propagación de enfermedades infecciosas y dividen la población en grupos como susceptibles, infectados y recuperados, definiendo probabilidades de transición entre ellos. Estos modelos permiten detectar la existencia de un flujo anómalo de información y predecir cuántas personas pueden verse expuestas o influenciadas a lo largo del tiempo. Sin embargo, tienen un carácter anónimo: no identifican quiénes son los individuos específicos que difunden la

desinformación ni las relaciones entre ellos. Así, su principal valor radica en ofrecer una visión agregada y macro del fenómeno, útil para identificar picos de difusión o evaluar el efecto de intervenciones generales (Martín García et al., 2024, pp. 22–23).

Por el contrario, las redes latentes de difusión son modelos generativos que representan explícitamente las interacciones entre los individuos de la red. A diferencia de los modelos epidemiológicos, permiten descubrir quién está propagando la información, cómo lo hace y con qué intensidad influye en otros. Las redes latentes de difusión eliminan la anonimidad al capturar la dirección y el peso de las relaciones entre cuentas o usuarios. Este nivel de detalle hace posible identificar actores clave (influencers o manipuladores), rutas de transmisión y estructuras comunitarias en la red, información crucial para diseñar estrategias de intervención dirigidas y detener campañas de desinformación de forma más eficaz (Martín García et al., 2024, p. 24).

En resumen, mientras los modelos epidemiológicos ofrecen una perspectiva global y estadística del fenómeno, útil para monitoreo general y simulación, las redes latentes de difusión proporcionan una visión granular y personalizada, permitiendo analizar en detalle quiénes propagan la desinformación y cómo se estructura esa difusión en la red social.

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?

El documento Luchando contra la desinformación mediante la inteligencia artificial subraya que la accesibilidad creciente de las herramientas de IA generativa está íntimamente ligada al aumento potencial de la desinformación. Gracias al desarrollo de modelos de código abierto y su disponibilidad en repositorios públicos, hoy en día cualquier persona con un ordenador doméstico potente y conocimientos básicos puede generar contenido engañoso realista. Esta democratización tecnológica ha reducido radicalmente las barreras de entrada, permitiendo la creación rápida y económica de textos, imágenes y audios manipulados de gran calidad. El riesgo asociado es que actores maliciosos pueden utilizar estas herramientas para lanzar campañas de desinformación más sofisticadas, masivas y difíciles de detectar, incrementando la infoxicación y erosionando la confianza pública (Martín García et al., 2024, p. 27).

Para mitigar este riesgo, el informe sugiere varias estrategias clave. En primer lugar, resalta la necesidad de desarrollar nuevos métodos ágiles y escalables de detección, capaces de contrarrestar la generación automática de bulos. También enfatiza la importancia de regular el uso de modelos de IA, especialmente aquellos de alto riesgo, para garantizar un acceso responsable y seguro. Además, se aboga por la implementación de sistemas de IA explicativa (XAI) que permitan entender y justificar las decisiones de los algoritmos de detección, fomentando la transparencia y la confianza pública. Finalmente, se destaca la relevancia de la cooperación internacional, la regulación legal y la alfabetización mediática para empoderar a los ciudadanos y reducir la efectividad de las campañas de desinformación (Martín García et al., 2024, pp. 27–28, 48–49).

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 identificadas si existen normativas en nuestro país similares.

El documento Luchando contra la desinformación mediante la inteligencia artificial destaca que el uso de Inteligencia Artificial (IA) para combatir la desinformación conlleva consideraciones éticas y de privacidad fundamentales. Entre los principales desafíos éticos se encuentra el riesgo de vigilancia masiva, el procesamiento no consentido de datos personales y la potencial vulneración de derechos fundamentales como la libertad de expresión y la privacidad. Para abordar estos retos, el texto enfatiza la importancia de limitar el análisis a información pública y de diseñar sistemas que eviten la identificación individual no consentida, centrando los esfuerzos en patrones agregados de difusión y análisis semántico del contenido (Martín García et al., 2024, p. 49).

En el ámbito normativo europeo, el informe menciona dos marcos clave. El Reglamento General de Protección de Datos (GDPR) impone estrictos requisitos sobre la recolección, el almacenamiento y el uso de datos personales, obligando a garantizar el consentimiento, la transparencia y la minimización de datos. Además, se menciona la propuesta de Ley de Inteligencia Artificial de la Unión Europea (EU AI Act), que establece un enfoque basado en niveles de riesgo para regular el desarrollo y despliegue de sistemas de

IA. Esta ley busca garantizar que los sistemas de IA sean seguros, transparentes y respetuosos de los derechos fundamentales, imponiendo requisitos más estrictos a los sistemas de alto riesgo, como los utilizados para la vigilancia o la toma de decisiones automatizadas con impacto significativo en las personas (Martín García et al., 2024, p. 49).

En cuanto a normativas nacionales en España, el país aplica directamente el GDPR como Estado miembro de la UE, complementado por la Ley Orgánica 3/2018, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD). Esta norma adapta y desarrolla el GDPR en el ordenamiento jurídico español, incluyendo garantías específicas sobre el uso ético de datos y derechos como la portabilidad, el olvido y la oposición a tratamientos automatizados. La LOPDGDD establece también principios de proporcionalidad y minimización que son especialmente relevantes para proyectos de IA destinados a combatir la desinformación, asegurando que se procesen solo los datos necesarios y con salvaguardas para los derechos de los usuarios.

En definitiva, el documento subraya que el desafío ético y legal consiste en diseñar sistemas de IA que sean eficaces contra la desinformación sin vulnerar la privacidad ni restringir injustificadamente la libertad de expresión, garantizando el cumplimiento de las normativas europeas y nacionales aplicables (Martín García et al., 2024, p. 49).

Referencias

Martín García, A., Panizo Lledot, Á., D'Antonio Maceiras, S. A., Huertas Tato, J., Villar Rodríguez, G., Anguera de Sojo Hernández, Á., & Camacho Fernández, D. (2024). Luchando contra la desinformación mediante la inteligencia artificial. Fundación BBVA.