1. ¿Cuál es la diferencia fundamental entre "misinformation" y *"disinformation"?

La diferencia fundamental radica en la intencionalidad y la veracidad de la información:

- **Misinformation** (información errónea) se refiere a datos falsos o inexactos que se comparten **sin intención de dañar**. Quien la difunde lo hace bajo la creencia de que es cierta. Ejemplo: compartir un remedio falso contra una enfermedad creyendo que funciona.
- Disinformation (desinformación) es información falsa, fabricada o manipulada con la intención deliberada de causar daño, manipular, confundir o engañar. Es intencionadamente maliciosa. Ejemplo: crear noticias falsas durante procesos electorales para influir en el voto.

A esta clasificación se suma un tercer concepto relevante:

• Malinformation, donde la información es veraz pero utilizada de manera manipulada o fuera de contexto para causar daño. Ejemplo: filtrar datos privados verdaderos de una persona para dañarla.

El texto enfatiza que en español usamos el término "desinformación" de forma genérica, lo que impide distinguir estos matices conceptuales fundamentales para entender el fenómeno y diseñar estrategias diferenciadas de combate.

2. ¿Qué tendencia preocupante se observa en España según el *Reuters Institute Digital News Report 2023*?

España presenta un fenómeno preocupante de **erosión acelerada en la confianza** pública hacia los medios de comunicación y el interés en la información verificada.

- En 2015, un 85% de la población manifestaba un alto o muy alto interés por las noticias.
- En 2023, este interés se desploma hasta el 51%, una reducción de 34 puntos porcentuales en menos de una década.

Simultáneamente, la desconfianza en los medios alcanza un récord del 40%, especialmente en la población joven (menores de 45 años).

Esto genera un fenómeno de "tormenta perfecta":

• Menos interés y menos confianza en los medios legítimos.

- Mayor exposición a fuentes alternativas no verificadas, principalmente redes sociales y aplicaciones de mensajería.
- Ecosistemas mediáticos donde la desinformación circula con mayor facilidad, afectando los procesos democráticos, la salud pública y la cohesión social.

3. ¿Cómo se comparan la velocidad y facilidad de difusión de noticias falsas frente a las verdaderas?

Según el influyente estudio de Vosoughi, Roy y Aral (2018) citado en el texto:

- Las noticias falsas se difunden significativamente más rápido, más lejos y con mayor profundidad que las verdaderas.
- El 1% de las fake news más exitosas alcanzó entre 1.000 y 100.000 personas, mientras que el 1% de las noticias verdaderas raramente superó las 1.000 personas.

Las causas principales son:

- Las noticias falsas suelen ser más novedosas, emocionales, sensacionalistas o impactantes, por lo que generan más interacciones (me gusta, compartidos, comentarios).
- Aprovechan los algoritmos de las plataformas que priorizan el contenido que genera mayor reacción, no el más veraz.
- Las redes funcionan como **amplificadores virales** que priorizan la difusión basada en la emocionalidad más que en la precisión.

4. ¿Qué ventaja clave ofrecen las redes latentes de difusión sobre los modelos epidemiológicos?

Las redes latentes de difusión representan un enfoque mucho más poderoso porque:

- Permiten identificar quién influye sobre quién, y cómo circula la información falsa en las redes sociales.
- Ofrecen una cartografía precisa de las dinámicas de influencia, modelando no solo la cantidad sino las relaciones directas entre usuarios.

• Facilitan localizar actores clave: emisores originales, amplificadores (influencers) y receptores pasivos.

En contraste, los **modelos epidemiológicos** (como el clásico modelo SIR) solo permiten observar patrones globales (cuántas personas están "infectadas" con la desinformación), pero no identifican ni actores ni rutas específicas de propagación.

Por lo tanto, las redes latentes son esenciales para:

- Diseñar intervenciones específicas, atacar nodos críticos.
- Comprender la estructura real de las campañas de desinformación, lo que permite contrarrestarlas de manera más efectiva.

5. ¿Qué son los "grandes modelos de lenguaje" y cuál es su principal riesgo?

• Son sistemas de inteligencia artificial entrenados con enormes volúmenes de datos textuales, capaces de generar, traducir, resumir y responder textos con coherencia humana. Ejemplos: GPT, BERT, LLaMA, Claude, etc.

Su principal riesgo en la desinformación es que:

- No comprenden la verdad ni la falsedad, solo predicen la palabra siguiente más probable.
- Son capaces de generar textos altamente convincentes, gramaticalmente correctos, pero completamente falsos.
- Facilitan que actores maliciosos produzcan campañas masivas de noticias falsas, bulos, artículos científicos inventados o discursos de odio, a bajo costo y sin necesidad de expertos.

Este riesgo es especialmente grave porque democratiza la capacidad de hacer desinformación profesional a cualquiera con acceso a estas herramientas.

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

- Antes se requerían recursos significativos (equipos especializados, conocimientos técnicos avanzados) para crear contenido falso sofisticado.
- Hoy, herramientas como ChatGPT, DALL-E, Stable Diffusion, ElevenLabs (audio) o Synthesia (video deepfake) permiten que cualquier persona, sin

conocimientos técnicos, pueda crear texto, imágenes, audios y videos falsos ultrarrealistas.

Esto conlleva que:

- El costo de entrada para la desinformación se reduce drásticamente.
- Aumenta la posibilidad de desinformación hiperpersonalizada, dirigida a públicos específicos.
- Se facilita la creación de campañas de astroturfing, manipulación social y fraude informativo sin precedentes.

7. ¿Qué son las "cajas negras" en IA explicativa y cuál es el desafío?

- Las "cajas negras" son modelos de IA cuyas decisiones son ininteligibles para los humanos, debido a su complejidad matemática y estadística (millones o billones de parámetros interconectados).
- Esto representa un problema crítico cuando la IA se usa en ámbitos sensibles (como la detección de fake news), porque no es posible saber por qué el sistema etiquetó un contenido como verdadero o falso.

El desafío es desarrollar **IA explicativa (XAI, Explainable AI)**, que permita entender, auditar y confiar en los procesos internos de los modelos, evitando sesgos, errores o manipulaciones opacas.

8. ¿Qué implicaciones tiene la *Inteligencia Artificial General (AGI)* para la desinformación?

- La AGI es un hipotético sistema de IA con capacidad cognitiva general, equivalente o superior a la inteligencia humana en cualquier tarea.
- En la lucha contra la desinformación, la AGI sería una herramienta poderosísima para:
 - o Detectar desinformación en tiempo real.
 - o Analizar texto, imágenes, audio y video simultáneamente.
 - Predecir y anticipar campañas de manipulación.

Sin embargo, también representaría un riesgo existencial si es utilizada para:

- Crear deepfakes indistinguibles de la realidad.
- Ejecutar operaciones psicológicas (PSYOPS) automáticas a escala global.
- Desestabilizar gobiernos, mercados o sociedades enteras mediante desinformación autónoma y autoaprendida.

9. ¿Qué normativas europeas importantes se mencionan?

- Reglamento General de Protección de Datos (GDPR): Marco legal para proteger los datos personales y la privacidad en Europa.
- Ley de Inteligencia Artificial de la Unión Europea (AI Act): Propuesta para regular la IA según su nivel de riesgo. Prohíbe sistemas de riesgo inaceptable (como manipulación subliminal) y regula el uso de IA en sectores críticos.

Estas normativas buscan garantizar que el uso de IA, incluso para combatir la desinformación, respete derechos fundamentales como privacidad, libertad de expresión y no discriminación.

10. ¿Cómo garantiza FacTeR-Check el cumplimiento de la normativa?

- FacTeR-Check opera exclusivamente sobre datos **públicamente disponibles** en redes sociales.
- No accede ni procesa conversaciones privadas, datos sensibles o información protegida.
- Incorpora medidas de anonimización y pseudonimización cuando los datos pudieran ser rastreables a individuos.
- Cumple rigurosamente con los principios del GDPR: minimización de datos, transparencia, seguridad y derecho al olvido.

11. Análisis de cómo la IA puede generar y combatir la desinformación

Uso para generar Uso para combatir

Texto: Fake news, discursos falsos Análisis semántico y verificación automática

Uso para generar

Uso para combatir

Imagen: Deepfakes, memes falsos Detección de imágenes manipuladas

Audio: Voces falsas, llamadas fake Reconocimiento de audio manipulado

Video: Videos hiperrealistas falsos Sistemas para detectar inconsistencias visuales

Bots: Difusión masiva automatizada Análisis de redes y detección de bots y trolls

La IA es una herramienta **dual**, tanto un riesgo como una solución, dependiendo de quién y cómo la utilice.

12. Papel de la IA explicativa (XAI)

- La XAI es esencial para que los sistemas de detección de desinformación sean:
 - o Auditable: se puede revisar cómo funciona.
 - o Transparente: las decisiones se entienden.
 - Confiable: los usuarios aceptan los resultados porque pueden ver la lógica detrás.
- Sin XAI, estos sistemas serían opacos y podrían ser rechazados social y jurídicamente.

13. Comparación profunda de modelos epidemiológicos y redes latentes

Característica	Modelos Epidemiológicos	Redes Latentes de Difusión
Tipo	Anónimo, basado en contagio	Personalizado, basado en influencia
Qué mide	Volumen global del fenómeno	Relaciones individuales
Precisión	Baja (macro)	Alta (micro)
Uso principal	Detección de anomalías	Identificación de actores clave
Ejemplo	SIR (susceptibles, infectados)	Análisis de cascadas de difusión

Característica Modelos Epidemiológicos Redes Latentes de Difusión

Requisito de datos Bajo

Alto (detalle por usuario)

Las redes latentes son el método más avanzado para el combate moderno de la desinformación.

14. Relación entre accesibilidad de IA y aumento de la desinformación + Estrategias

- Accesibilidad = democratización del riesgo.
- Hoy cualquiera con una PC decente puede crear noticias falsas, videos deepfake, voces clonadas, etc.

Estrategias sugeridas:

- Legislación firme (AI Act, GDPR).
- Desarrollo de sistemas de IA explicativa y verificadores automáticos.
- Fomento de la alfabetización mediática y digital en la población.
- Alianzas público-privadas para crear estándares y filtros tecnológicos.

15. Ética y privacidad en el uso de IA

• Ética:

- o Transparencia algorítmica.
- No discriminación ni sesgos.
- o Responsabilidad y trazabilidad.

• Privacidad:

- Uso de datos estrictamente públicos.
- Aplicación de principios de minimización y anonimización.
- o Respetar derechos fundamentales, incluida la libertad de expresión.

Cualquier uso de IA para combatir desinformación debe ser compatible con los principios democráticos y los derechos humanos.