

ÍNDICE

I. - INTELIGENCIA ARTIFICIAL. CONTEXTO Y RIESGOS

1. El contexto técnico y social que explica la recuperación de la inteligencia artificial
 1. 1. Big Data
 1. 2. Internet de las cosas
 1. 3. Blockchain o tecnología de bloques distribuidos
2. El problema de la definición de la inteligencia artificial
 2. 1. La inteligencia artificial como ciencia
 2. 2. El problema de la definición de la inteligencia artificial
 2. 3. Los diferentes grados de la inteligencia artificial: IA Fuerte y blanda
3. Ciclo de vida y técnicas de IA
 3. 1. Machine learning o aprendizaje automático
 3. 2. Deep learning o aprendizaje profundo
 3. 3. Aprendizaje semiautomático o reforzado
4. Riesgos específicos de la IA
 4. 1. Ataques dirigidos al funcionamiento del modelo
 - A) Envenenamiento de datos
 - B) Ataques adversarios de machine learning y deep learning
 4. 2. Ataques dirigidos a la privacidad y protección de los datos utilizados
 4. 3. Ataques dirigidos al ecosistema de IA

II. - INICIATIVAS Y ENFOQUES ÉTICO-JURÍDICOS DE ÁMBITO INTERNACIONAL Y COMUNITARIO

1. Principales iniciativas de vocación internacional
 1. 1. La OCDE y los principios sobre inteligencia artificial
 1. 2. El Consejo de Europa
 - A. El Convenio 108 del Consejo de Europa
 - B. La regulación jurídica del perfilado en el Consejo de Europa
 - C. Lineamientos sobre procesamiento de información y Big Data
 - D. La declaración sobre capacidades manipulativas de los procesos algorítmicos y la recomendación sobre el impacto de los sistemas algorítmicos en los derechos humanos
2. Autorregulación y normas éticas de vocación internacional
 2. 1. Los principios Asilomar
 2. 2. Recomendación sobre la ética de la inteligencia artificial de la UNESCO
3. Enfoques regulatorios de algunas potencias: China y Estados Unidos

3. 1. El enfoque norteamericano en materia de IA: liderazgo corporativo y regulación “light-touch”
3. 2. El enfoque chino: orientación estatal y regulación gradual
3. 3. La construcción de la política europea sobre inteligencia artificial: Enfoque basado en derechos bajo un trinomio normativo
4. La propuesta ética europea: Inteligencia artificial fiable
5. El mandato comunitario de estandarización en materia de inteligencia artificial

III. - BASES PARA EL DISEÑO Y APLICACIÓN DE UN MARCO JURÍDICO COMUNITARIO PARA LA INTELIGENCIA ARTIFICIAL

1. Regulación a través de otras normas e insuficiencia de la respuesta
2. La estrategia comunitaria sobre la inteligencia artificial: Un enfoque sostenible basado en los riesgos y los derechos
3. El modelo regulatorio de la UE para la inteligencia artificial: Opciones y características
 3. 1. Opciones regulatorias respecto a la IA. La cuestión de la intensidad de la intervención normativa
 3. 2. Principales características del modelo regulatorio comunitario de la IA
4. Principios aplicables para conciliar estándares elevados de protección con la innovación responsable (principios para diseñar un marco de IA)
 4. 1. Principios relacionados con el diseño del marco y el enfoque regulatorio
 - A. Neutralidad tecnológica
 - B. Principio de innovación
 - C. Principio de precaución
 4. 2. Principios dirigidos a recoger protecciones legales desde el diseño
 - A. IA centrada en el ser humano
 - B. Privacidad, protección de datos y seguridad por diseño
 - C. Competencia por diseño

IV. - TÉCNICAS Y GARANTÍAS ESPECÍFICAS PARA EL DISEÑO Y APLICACIÓN DEL MARCO COMUNITARIO DE INTELIGENCIA ARTIFICIAL

1. La clasificación de las aplicaciones en atención al riesgo y su régimen jurídico
2. Aplicaciones restringidas o prohibidas
 2. 1. Sistemas y aplicaciones de manipulación o explotación
 2. 2. Sistemas de clasificación social
 2. 3. Sistemas de identificación biométrica en tiempo real en espacios de acceso público con fines de aplicación de la ley
3. Aplicaciones y sistemas de alto riesgo
 3. 1. Clasificación de sistemas de alto riesgo
 - A. Sistemas de AI diseñados como componentes de seguridad de otros productos
 - B. Sistemas de alto riesgo recogidos en el anexo III
 3. 2. Requisitos horizontales de los sistemas de IA de alto riesgo
 - A. Sistema de gestión del riesgo (SGR)

- B. Gobernanza de los datos
 - C. Documentación técnica
 - D. Registros
 - E. Transparencia
 - F. Vigilancia humana
 - G. Precisión, solidez y ciberseguridad
- 3. 3. Sujetos y obligaciones relacionadas con sistemas de alto riesgo
 - 3. 4. Base de datos y registro de aplicaciones de alto riesgo
- 4. Aplicaciones no consideradas de alto riesgo
 - 5. Obligaciones transversales de transparencia para sistemas que interactúen con humanos

V. - LAS ESTRUCTURAS DE GOBERNANZA, PROCEDIMIENTOS DE EVALUACIÓN DE LA SEGURIDAD DE LOS SISTEMAS Y POLÍTICAS DE APOYO

- 1. Estructuras de gobernanza de la IA
 - 1. 1. Comité Europeo de Inteligencia Artificial. Composición, competencias y funciones
 - 1. 2. Autoridades nacionales. Designación y competencias
 - 1. 3. Las estructuras de apoyo a la política y regulación de IA
 - 1. 4. Organismos notificados y organismos de evaluación de la conformidad
- 2. Procedimientos de evaluación y salvaguardia
 - 2. 1. Procedimientos de evaluación de la conformidad. Autocertificación y evaluación por tercera parte
 - 2. 2. Exención del procedimiento de evaluación de la conformidad y nueva evaluación por modificación sustancial
- 3. Procedimiento y medidas post-comercialización o de vigilancia del mercado
 - 3. 1. Medidas de intercambio de información en casos de incidentes y fallos de funcionamiento
 - 3. 2. Procedimiento de salvaguardia en casos de sistemas que planteen riesgo grave a nivel nacional
 - 3. 3. Procedimiento de salvaguardia en casos de sistemas que planteen riesgo grave a nivel comunitario
 - 3. 4. Procedimiento de sistemas de IA conformes que presenten riesgos
 - 3. 5. Procedimiento en caso de incumplimiento de obligaciones formales
- 4. Política y medidas de fomento a la innovación: Espacios controlados de prueba

BIBLIOGRAFÍA