ÍNDICE

INTRODUCCIÓN

La transformación de la privacidad

El auge del dataísmo y los riesgos de la IA en la privacidad

El papel del derecho en un mundo digital

PARTE I. LA IA Y LA PRIVACIDAD: ORÍGENES Y EVOLUCIÓN

CAPÍTULO 1. DE LAS HUELLAS DIGITALES A LA INTELIGENCIA ARTIFICIAL: EL VIAJE DE LOS DATOS Y LA PRIVACIDAD

1. Introducción: El cerebro detrás de la revolución tecnológica

2. Orígenes de la inteligencia artificial: De Turing a los algoritmos modernos

3. El fascinante mundo de la Inteligencia Artificial: Descifrando sus secretos

4. Tipos de inteligencia artificial: Desde asistentes hasta máquinas superinteligentes

5. ¿Cómo funciona la inteligencia artificial? Los algoritmos y los riesgos asociados…

6. La economía del big data: datos como moneda de cambio

    6.1. Los distintos rostros de los datos y su relevancia en el marco del Reglamento de IA

    6.2. La paradoja de Pulgarcito: Migajas digitales fuera de control

7. Retos y peligros de la inteligencia artificial: Una mirada desde el impacto humano

    7.1. Los datos como moneda de cambio: ¿A qué costo?

    7.2. La sombra de la vigilancia masiva

    7.3. Burbujas informativas y polarización: La paradoja de la personalización

    7.4. Más allá del individuo: El impacto colectivo de la IA

8. Visión antropocéntrica de las directrices éticas para una IA fiable: la IA desde la dignidad de la persona

    8.1. La visión ética

    8.2. Hacia una privacidad más justa y equitativa

9. Inteligencia artificial en España: Oportunidades y desafíos

10. Conclusiones iniciales

CAPÍTULO 2. LA PRIVACIDAD EN PERSPECTIVA: DEL REFUGIO MORAL A LA PROTECCIÓN LEGAL

1. Introducción

2. Grecia, Roma y la transición desde el cristianismo a la Edad Moderna

3. La Edad Moderna

4. El fin de la Edad Moderna

5. De la sociedad industrial al nacimiento del genuino right to privacy

6. El «right to privacy» de Warren y Brandeis y su posterior desarrollo doctrinal, jurisprudencial y normativo en Norteamérica

7. La recepción del derecho a la intimidad en los textos normativos supranacionales

8. El derecho a la intimidad en el plano nacional

9. Una nueva necesaria comprensión de la privacidad

CAPÍTULO 3. DE LA PLAIN VIEW DOCTRINE A LA TEORÍA DEL MOSAICO: REDEFINICIÓN DEL RIGHT TO PRIVACY Y SITUACIÓN PREVIA A LA IA

1. Introducción

    1.1. La intimidad: un concepto en plena evolución

    1.2. La distinción intimidad-privacidad

    1.3. La nueva dimensión de la privacidad en la era digital

    1.4. La nueva caja fuerte de los datos

2. La plain view doctrine como excepción y su adaptación al entorno digital

    2.1. Orígenes y fundamentos en la jurisprudencia norteamericana

    2.2. Restricciones iniciales y jurisprudencia relevante

    2.3. Problemáticas en el entorno digital

3. De Olmstead a Carpenter: la evolución de la reasonable expectation of privacy

    3.1. Primera fase: intrusión física como requisito

    3.2. Katz v. United States (1967): la protección de la persona

    3.3. La third-party doctrine y sus controversias

    3.4. Kyllo, Jones, Riley y la introducción de la teoría del mosaico

4. Carpenter v. United States (2018) y la reconfiguración de la third-party doctrine

    4.1. “Vayamos al caso”: hechos y debate legal

    4.2. El golpe en Europa: la anulación de la Directiva 2006/24/CE

5. Recepción en España: evolución doctrinal y jurisprudencial hacia el entorno digital

    5.1. Fundamentos constitucionales de la privacidad en España

    5.2. La adopción de la plain view doctrine y la expectativa razonable en la jurisprudencia del Tribunal Supremo

    5.3. “Teoría de la activación”: por qué no forma parte de nuestra doctrina constitucional

    5.4. Entorno digital y proceso penal: límites a la exploración indiscriminada y deber de acotación

    5.5. Derecho al olvido, consentimiento y reedición de informaciones antiguas

    5.6. Videovigilancia, comunicaciones y “expectativa” en el trabajo: el espejo europeo

5.7. Vigilancia prolongada, geolocalización y la “teoría del mosaico” en clave europea

5.8. Retorno al caso “ventanas abiertas” y reglas de oro

5.9. Apunte final

6. Conclusiones: la caja fuerte de la privacidad

PARTE II. EL ECOSISTEMA DE DATOS Y EL CAPITALISMO DE VIGILANCIA

CAPÍTULO 4. EL CAPITALISMO DE VIGILANCIA: CÓMO LAS EMPRESAS EXPLOTAN TUS DATOS

1. Introducción al capitalismo de vigilancia

2. La revolución digital y su paradoja

3. El impacto de la sociedad vigilada: ¿Google nos lee el cerebro?

4. Métodos de recopilación y monetización de datos personales por empresas

4.1. Métodos de recopilación de datos

4.2. Métodos de monetización de datos

5. Casos destacados: Cambridge Analytica y el uso político de los datos

6. El Fin del Capitalismo de Vigilancia: La Necesidad de Devolver los Datos al Ciudadano

7. ¿Cómo Pueden las Tecnológicas Adaptarse a este Cambio?

8. Conclusión: Un Nuevo Pacto Digital

CAPÍTULO 5. ¿QUÉ NECESITA LA INTELIGENCIA ARTIFICIAL PARA FUNCIONAR?

1. Introducción: El mundo de la IA se ha judicializado

2. El volumen de datos: el motor de la IA

2.1. ¿Cómo se buscan y procesan los datos?

2.2. La escala masiva: ¿Cuánto es suficiente?

3. Los datos deben ser diversos y precisos para garantizar resultados confiables

3.1. La importancia de la diversidad en los datos

3.2. La precisión de los datos: el motor de la confiabilidad

3.3. Cómo garantizar diversidad y precisión en los datos

3.4. Implicaciones legales y éticas

4. Los algoritmos y su naturaleza de “caja negra”: hacia un compliance algorítmico

5. El derecho a los datos de carácter personal como derecho fundamental: del habeas data al derecho al olvido

CAPÍTULO 6. CONSENTIMIENTO EN LA ERA DE LA INTELIGENCIA ARTIFICIAL: DEL HOTEL AL ALGORITMO

1. La Fatiga del Consentimiento: el clic automático

    1.1. Paradojas del consentimiento

2. Doctrina y Evolución del Consentimiento

    2.1. De lo estático a lo dinámico

    2.2. Principios fundamentales

3. Legislación y praxis española

    3.1. El Consentimiento en la Protección de Datos en España: Un Marco Regulatorio en Evolución

    3.2. La Trazabilidad de los Datos en la Inteligencia Artificial: Un Pilar de Transparencia y Control

    3.3. La praxis española en materia de consentimiento informado: Hacia una protección efectiva en la era digital

4. El Consentimiento en la Era de la IA: Replanteando la Protección de Datos en un Mundo Inteligente

5. Conclusión: Reinventando el Consentimiento en la Era de la IA

PARTE III. IMPACTOS DE LA IA EN LOS DERECHOS FUNDAMENTALES

CAPÍTULO 7. IA Y DERECHOS HUMANOS: UNA RELACIÓN EN TENSIÓN

1. Introducción

2. El significado de los “derechos humanos”

3. Las “generaciones de derechos” como criterio hermenéutico

    3.1. La primera generación de derechos

    3.2. La segunda generación de derechos

    3.3. La tercera generación de derechos

    3.4. Más allá de la tercera generación de derechos

4. El papel protagonista del art. 18.4 CE

CAPÍTULO 8. MÁS ALLÁ DE LA PRIVACIDAD: OTROS DERECHOS FUNDAMENTALES BAJO AMENAZA

1. Introducción

2. Granjas de troles, fake news y derecho al honor

3. La construcción de la realidad

4. La libertad de expresión e información y la mentira

5. La mentira que excede de la libertad de expresión

6. La secretaría técnica de la Fiscalía General del Estado y su informe sobre el “tratamiento penal de las «fake news»”

7. Los riegos de la criminalización de la palabra

8. El sanedrín de las tecnológicas

CAPÍTULO 9. PRIVACIDAD Y TECNOLOGÍA EN NUESTRA PRAXIS JUDICIAL

1. Estados Unidos: Donde la privacidad se encuentra con la tecnología

    1.1. Katz v. United States (1967): La cabina telefónica que redefinió la privacidad

    1.2. Carpenter v. United States (2018): Nuestros teléfonos, ¿extensiones de nosotros mismos?

    1.3. Facebook, Inc. v. Duguid (2021): Marcando los límites del marketing digital

    1.4. Roe v. Wade (1973) y su impacto en la privacidad: El derecho a la intimidad

2. Europa: El guardián de la privacidad en la era digital

    2.1. Google Spain v. AEPD y Mario Costeja González (2014): El derecho a ser olvidado

    2.2. Schrems I (2015) y Schrems II (2020): La lucha por la soberanía digital

    2.3. Digital Rights Ireland (2014): Límites a la retención de datos

    2.4. Big Brother Watch v. United Kingdom (2021): Un golpe al corazón de la vigilancia masiva

3. España: Pionera en la defensa de la privacidad

    3.1. Tecnologías de control en manos del Estado

    3.2. La evolución doctrinal y jurisprudencial

    3.3. Investigaciones privadas y la transparencia informativa

    3.4. Conclusión: Tecnologías de control y derechos fundamentales

    3.5. Caso LaLiga App (2020): Cuando la tecnología se extralimita

4. Los problemas asociados a las cadenas de redifusión de datos

5. La criminalización de las cadenas de envío

6. El caso Celebgate como expresión de la tensión de la privacy

7. Y si las sentencias condenatorias llegan, las indemnizaciones son escasas

    7.1. Breves consideraciones sobre la responsabilidad civil por las intromisiones ilegítimas en la intimidad

    7.2. Las ridículas (o inexistentes) indemnizaciones en la jurisdicción penal

8. Conclusiones

PARTE IV. PROPUESTAS PARA UN MARCO NORMATIVO GLOBAL

CAPÍTULO 10. HACIA UNA REGULACIÓN ÉTICA Y GLOBAL DE LA IA

1. Introducción: La IA, la nueva tragedia de los comunes
    - 1.1. La IA como bien común: ¿Gestión privada, estatal o comunitaria?
    - 1.2. La necesidad de estándares internacionales para la IA
2. Elementos clave: ética, transparencia y rendición de cuentas
    - 2.1. Ética como pilar central
    - 2.2. Transparencia como eje de confianza
    - 2.3. Rendición de cuentas como principio rector
    - 2.4. El papel de la gobernanza global
3. Evaluaciones de impacto ético y modelos de implementación
    - 3.1. Evaluaciones de impacto ético como herramienta clave
    - 3.2. Modelos de implementación: organismos regulatorios internacionales
    - 3.3. ¿Cómo involucrar a múltiples partes interesadas en la regulación?
    - 3.4. Capacidades para países en vías de desarrollo
    - 3.5. El papel de las organizaciones internacionales

CAPÍTULO 11. DATA NEXUS JURIS: UN MARCO JURÍDICO PARA LA PRIVACIDAD EN LA ERA DE LA IA

1. Introducción: Los datos como masa grasienta y el efecto spillover
2. Privacidad como derecho colectivo y bien común
    - 2.1. Dimensiones colectivas de la privacidad
    - 2.2. Privacidad colectiva frente a la inteligencia artificial
    - 2.3. Privacidad como instrumento de resistencia colectiva
    - 2.4. Del secreto profesional humano al “privilegio conversacional con IA”
3. Introducción al concepto del Data Nexus Juris: hacia la protección del entorno. Una “nouvelle vague” del habeas data
4. Diferencias y evolución desde el habeas data
    - 4.1. Desafíos prácticos en la aplicación del Data Nexus Juris
    - 4.2. Resistencia de las corporaciones tecnológicas
    - 4.3. Acceso desigual a recursos y tecnologías
    - 4.4. Educación y concienciación
    - 4.5. Impacto potencial en la gobernanza global de datos
    - 4.6. Protección frente a riesgos globales

4.7. Innovación responsable

5. La Caja Fuerte Digital de Datos en el Marco del Data Nexus Juris

5.1. Introducción

5.2. Definición Jurídica de la Caja Fuerte Digital de Datos

5.3. Morada Informática como Base del Data Nexus Juris

6. Análisis Global y Jurídico de la Caja Fuerte Digital de Datos

6.1. Regulaciones Existentes y Cómo la Caja Fuerte Digital las Complementa

7. Bases Doctrinales, Políticas y Sociológicas

8. El Consentimiento Digital: De la Ficción Jurídica a la Autodeterminación Real

8.1. El Consentimiento en la Era del Capitalismo de Vigilancia

8.2. El Consentimiento Granular: Un Nuevo Modelo para la Autodeterminación Informativa

8.3. Tecnologías para Garantizar un Consentimiento Real

8.4. Regulaciones Necesarias para un Consentimiento Digital Justo

9. La confidencialidad del chatbot

10. Propuesta de Regulación

11. El derecho penal como última ratio del sistema de protección

12. Conclusión

CAPÍTULO 12. LA IA Y LA EVOLUCIÓN DE LOS DELITOS EN LA ERA DIGITAL

1. Introducción: La nueva era del crimen impulsado por la inteligencia artificial

2. Nuevas formas de violación de la intimidad: vigilancia masiva y rastreo

2.1. Vigilancia masiva y reconocimiento facial

2.2. Doxing automatizado y el uso de IA: amenazas a la privacidad y la seguridad

2.3. Análisis y correlación de datos personales: el poder de los algoritmos en la era de la IA

2.4. Deepfakes: Violaciones a la intimidad y retos éticos en la era de la inteligencia artificial

2.5. Explotación de datos biométricos: La vulnerabilidad de nuestra identidad más íntima

2.6. Vigilancia de dispositivos personales: La nueva frontera de la invasión digital

2.7. Tipos penales que deben redefinirse

3. Redefinición de delitos como el acoso y la extorsión en la era de la inteligencia artificial

3.1. Acoso digital: Bots, automatización y vigilancia personalizada

3.2. Extorsión personalizada: La precisión de la IA para manipular

4. Uso de deepfakes para difamación y chantaje: Una amenaza emergente en la era de la IA

4.1. El desafío técnico: La complejidad de identificar un deepfake

4.2. Propuestas para abordar el uso malicioso de deepfakes

5. Propuesta Unificada y Recomendaciones Finales

EPÍLOGO. CUANDO LA TECNOLOGÍA REDEFINE LO HUMANO, EL PODER Y LA ÉTICA

BIBLIOGRAFÍA