

# ÍNDICE

## INTRODUCCIÓN

### Capítulo I. ELEMENTOS CLAVE DE UN NUEVO PARADIGMA: LA 4.<sup>a</sup> REVOLUCIÓN INDUSTRIAL.

#### I. IDEA INDIVIDUAL E IDEA SOCIAL DEL DERECHO

1. Un derecho justo y un derecho válido: moralidad y ética en el derecho
2. La seguridad jurídica como ingrediente fundamental
3. La adaptabilidad del derecho y el intervencionismo público

#### II. PRIVACIDAD

1. Introducción histórica
2. Interpretación constitucional. Alcance y límites del derecho

#### III. EL SECTOR ASEGURADOR

1. El riesgo y su incertidumbre
2. Condiciones generales, particulares y limitativas del seguro
3. Principio de solidaridad
4. Nuevas necesidades que asegurar

#### IV. NOTAS CARACTERÍSTICAS DE LA NORMATIVA DE REFERENCIA: ESPECIAL IMPACTO DEL DEBER DE INFORMACIÓN

1. Regulación paternalista o libertaria
2. Situación regulatoria del deber de información en España

### Capítulo II. LA INTELIGENCIA ARTIFICIAL EN EL SECTOR ASEGURADOR

#### I. DEFINICIÓN DE DATO PERSONAL

#### II. CONCEPTO DE INTELIGENCIA ARTIFICIAL Y BIG DATA

1. Introducción. Nuevas fuentes de datos
2. La IA
  - 2.1. *Aprendizaje automático*
  - 2.2. *IA fuerte e IA débil*
  - 2.3. *Inteligencia Artificial y Big Data en el sector asegurador. Ventajas asociadas a los usos y soluciones empleadas*

### Capítulo III. EL USO DE LA INTELIGENCIA ARTIFICIAL EN EL SECTOR ASEGURADOR Y SUS RIESGOS PARA LA PROTECCIÓN DE DATOS PERSONALES

#### I. INTRODUCCIÓN.

#### II. RIESGOS PARA EL INDIVIDUO COMO PERSONA FÍSICA

1. El uso inadecuado de los datos: cálculo de la prima a través de factores ajenos al riesgo
2. Un gobierno inadecuado del dato como principal causante de brechas de seguridad.
3. Datos excesivos: la problemática de los datos de categoría especial y de los datos inferidos
4. Acceso indiscriminado a los propios datos y de terceros
5. Monitorización, seguimiento y perfilado constante de individuos.
6. La modificación del comportamiento y su impacto en la autonomía de la voluntad

7. Dificultad en el control de los datos: el principio de limitación del plazo de conservación, terceros destinatarios y transferencias internacionales
  - 7.1. *Número de intervinientes o destinatarios de los datos personales*
  - 7.2. *El plazo de conservación de los datos personales*
8. Correlaciones y sesgos: vicios de exactitud
9. Dificultad de transparencia e inteligibilidad en la IA: el reto de la explicabilidad y las Black Boxes
10. Consentimiento viciado: negociación previa y modificación contractual sobrevenida.
  - 10.1. *El consentimiento en la fase precontractual*
  - 10.2. *El consentimiento ante las modificaciones contractuales sobrevenidas*
11. Asimetría entre la posición de consumidor y empresario

### III. RIESGOS PARA LA ENTIDAD ASEGURADORA COMO DESTINATARIA DEL RGPD

1. La conculcación del principio de legalidad y de seguridad jurídica en la nueva normativa
  - 1.1. *Punto de partida: principio de legalidad como elemento clave de un Estado de Derecho*
  - 1.2. *Encargados de tratamiento: la posición de garante del Responsable del Tratamiento*
  - 1.3. *El contenido de la información sobre la lógica aplicada*
  - 1.4. *Inseguridad jurídica derivada de la propia actuación de las administraciones públicas*
2. El amplio margen sancionador
3. Vulneración del secreto empresarial y fraudes a la aseguradora
4. La compleja asegurabilidad de nuevos riesgos asociados a la IA
5. Situación de monopolio: dificultad para mantener un mercado competitivo

### IV. RIESGOS SISTÉMICOS. SOCIEDAD Y ESTADO

1. Asesoramiento inadecuado en la contratación y responsabilidad derivada
2. La determinación del grado de intervención humana para asegurar la supervisión
3. Problemas de corte ético-moral. Discriminación y conciencia de la IA
4. Dificultad en la determinación del grado de control e intervención estatal ante la IA
5. Determinación de responsabilidad administrativa: la sanción económica
6. Incierta clasificación de niveles de riesgo de la IA
7. Comercialización y patrimonialización de los datos personales
8. Retos para el principio *non bis in idem*: duplicidad de autoridades, controles y regulación
  - 8.1. *Plano nacional*
  - 8.2. *Plano europeo*
9. La asegurabilidad de los datos personales en el metaverso
10. Responsabilidad civil
  - 10.1. *Opacidad y autonomía de los sistemas de IA*
  - 10.2. *Clasificación de la IA: su consideración como producto*
  - 10.3. *RGPD y LIA: clasificación y compatibilidad de la responsabilidad civil*
  - 10.4. *Compleja y opaca cadena de responsables e intervinientes en sistemas de IA . 299*
  - 10.5. *Dificultades para aplicar la normativa de productos defectuosos*
    - 10.5.1. *La inaplicabilidad de las causas de exoneración previstas en el art. 140 RD 1/2007*
    - 10.5.2. *La diversidad de términos y conceptos para designar al responsable 302*
    - 10.5.3. *Daños morales*
    - 10.5.4. *Uso privativo: ámbito restringido de aplicación del TRLGDCU*
    - 10.5.5. *Producto defectuoso y prueba del defecto*
    - 10.5.6. *Plazo para la manifestación de ausencia de conformidad y plazo para reclamar el daño*
  - 10.6. *Determinación y clasificación de los sistemas de IA de alto riesgo*
  - 10.7. *Diferencias entre la propuesta del Parlamento y la Directiva de la Comisión*
  - 10.8. *Seguro de responsabilidad civil obligatorio*

## Capítulo IV. INTERPRETACIÓN DE LAS OBLIGACIONES NORMATIVAS DE IA Y PROTECCIÓN DE DATOS PARA LA REDUCCIÓN DE RIESGOS EN EL SECTOR ASEGURADOR

### I. ASPECTOS GENERALES DE LA NORMATIVA ACTUAL

1. Enfoque actual: obligación de medios
2. Ámbito subjetivo de aplicación de la normativa.

## II. OBLIGACIONES ESPECÍFICAS DE LA NORMATIVA DE INTELIGENCIA ARTIFICIAL.

1. Sistemas de alto riesgo y plazo para su adecuación
2. Elementos y definiciones clave para el entendimiento de la LIA
3. Obligaciones concretas del responsable del despliegue
  - 3.1. *Utilización y vigilancia del sistema de acuerdo con las instrucciones de uso que acompañen al mismo*
  - 3.2. *Vigilar el funcionamiento del sistema de IA encomendando la supervisión humana a personas físicas con competencia, formación y autoridad necesarias .*
  - 3.3. *En caso de ejercer control sobre los datos de entrada que alimentan el algoritmo, deberá asegurarse la pertinencia de estos y de que sean suficientemente representativos para la finalidad prevista para el sistema de IA*
  - 3.4. *Obligaciones de comunicación ante la detección de determinados riesgos generales o incidentes graves o defectos de funcionamiento*
  - 3.5. *Conservar por tiempo adecuado los archivos de registro generados por los sistemas de IA siempre que los mismos se encuentren bajo su control*
  - 3.6. *Realización de una evaluación de impacto en materia de protección de datos personales empleando para ello la información que el proveedor está obligado a facilitar*

## III. OBLIGACIONES ESPECÍFICAS DE LA NORMATIVA DE RGPD

1. Cumplimiento de los principios básicos
  - 1.1. *Licitud*
  - 1.2. *Lealtad y transparencia*
    - 1.2.1. *Qué debe entenderse por lógica aplicada*
    - 1.2.2. *Cómo facilitar información sobre sistemas que han sido calificados de poco transparentes (black box) incluso para aquellos que los han desarrollado*
    - 1.2.3. *Dónde y en qué momento debe ponerse a disposición del interesado dicha información*
  - 1.3. *Limitación de la finalidad*
  - 1.4. *Minimización de datos*
  - 1.5. *Exactitud*
  - 1.6. *Conservación*
  - 1.7. *Integridad y confidencialidad*
  - 1.8. *Proactividad*
2. Garantizar los derechos de los usuarios: derecho de acceso, supresión y no ser objeto de elaboración de perfiles
  - 2.1. *Acceso*
  - 2.2. *Rectificación*
  - 2.3. *Supresión*
  - 2.4. *Derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles que produzca efectos jurídicos en él o le afecte significativamente de modo similar*
3. Adopción de medidas de seguridad técnicas y organizativas
  - 3.1. *Privacidad desde el diseño y por defecto*
  - 3.2. *Existencia de políticas y procedimientos*
  - 3.3. *Análisis de riesgos y evaluación de impacto*
    - 3.3.1. *Cómo debo llevar a cabo un análisis de riesgos*
    - 3.3.2. *Cómo debo llevar a cabo una EIPD*
    - 3.3.3. *Cómo saber que un tratamiento entraña un alto riesgo que precisa de EIPD*
  - 3.4. *Procedimiento de notificación de brechas de seguridad.*
    - 3.4.1. *Cuando nos encontramos ante una violación de seguridad*
    - 3.4.2. *Cuando debe notificarse a la Autoridad de protección de datos e, incluso, comunicar a los interesados.*
    - 3.4.3. *Desde qué momento debe computarse el plazo para notificar la brecha de seguridad.*
  - 3.5. *Auditorías*
4. Nombramiento obligatorio de un DPO para las aseguradoras
  - 4.1. *Qué rol desempeña esta figura en una organización*
  - 4.2. *La obligatoriedad de su nombramiento para una entidad aseguradora*
  - 4.3. *Los conocimientos específicos que pueden ser exigidos*

5. Contratos de encargado de tratamiento y evaluación de los mismos: los «gigantes tecnológicos» y las transferencias internacionales y garantías
  - 5.1. *Imposibilidad de negociar determinadas cláusulas contractuales que vienen impuestas por la cuota de mercado que representan*
  - 5.2. *Dificultad para extraer información suficiente que permita evaluar al Encargado del tratamiento*
  - 5.3. *Dificultad a la hora de controlar dónde se encuentran los datos y con quién se comparten*
6. La figura de los códigos de conducta y las certificaciones
  - 6.1. *Códigos de conducta*
  - 6.2. *Mecanismos de certificación*
7. Contratación de seguros específicos para la cobertura de los riesgos derivados de incumplimiento y/o ataques de terceros
  - 7.1. *Entidad aseguradora como proveedor*
  - 7.2. *Entidad aseguradora como cliente 0*
8. Los programas de Compliance

## **CONCLUSIONES**

## **REFERENCIAS BIBLIOGRÁFICAS**