INCIDENCIA DE LA PROTECCIÓN DE DATOS EN EL USO DE LA INTELIGENCIA ARTIFICIAL

Agencia Tributaria

VII JORNADA REVISTA GABILEX

ALEJANDRO BONIS SANZ
Subdirector de Organización y Asistencia Jurídica
Servicio Jurídico

Toledo - 17 de octubre de 2024

INCIDENCIA DE LA PROTECCIÓN DE DATOS EN EL USO DE LA INTELIGENCIA ARTIFICIAL

1. Introducción
2. Conceptos
3. Marco normativo
   - Normativa interna
   - Normativa internacional
   - “Soft Law”
   - Jurisprudencia
4. Requisitos jurídicos de la protección de datos en el desarrollo y uso de sistemas de IA
5. Régimen jurídico de la IA. Principales desafíos que plantea la protección de datos.
   - El Reglamento IA
   - Transparencia en la IA
   - Gestión de Riesgos EIPD
   - Gobernanza de datos
6. Ejemplos y jurisprudencia relevante
7. Conclusiones

Riesgos jurídicos en el uso de Sistemas de Inteligencia Artificial por Administraciones Públicas

CONCEPTOS JURÍDICOS

CONCEPTOS JURÍDICOS

BIG DATA

Resolución del Parlamento Europeo, de 14 de marzo de 2017, sobre las implicaciones de los macrodatos en los derechos fundamentales: privacidad, protección de datos, no discriminación, seguridad y aplicación de la ley

Considerando que el concepto de macrodato se refiere a la **recopilación, análisis y acumulación constante de grandes cantidades de datos**, incluidos datos personales, procedentes de diferentes fuentes y **objeto de un tratamiento automatizado** mediante algoritmos informáticos y avanzadas técnicas de tratamiento de datos, utilizando tanto datos almacenados como datos transmitidos en flujo continuo, **con el fin de generar correlaciones, tendencias y patrones** (analítica de macrodatos)

BIG DATA

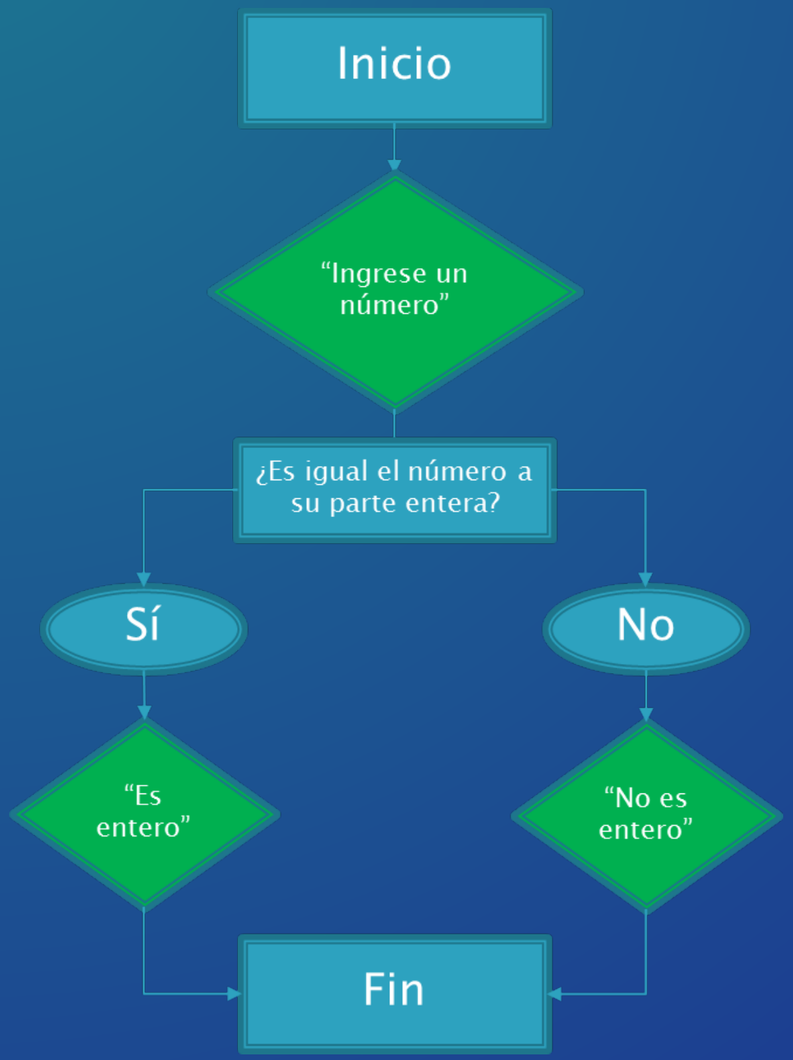

Big Data
Activo
Recopilación y análisis de una gran cantidad de datos, mediante un tratamiento automatizado a través de algoritmos informáticos
Finalístico
Generar correlaciones, tendencias y patrones
Minería de datos o analítica de macrodatos

ALGORITMO

Conjunto ordenado y finito de operaciones que permite hallar la solución de un problema

Algoritmo	Algoritmo matemático (diagrama de flujo)
	Algoritmo informático o seudocódigo de programación
	Código de programación (lenguaje de programación)
	Código binario

ALGORITMO



¿Es el número entero?

1. Solicitar al usuario que ingrese un número.
2. Leer y almacenar el número ingresado.
3. Verificar si el número es igual a su parte entera (sin decimales).
4. Si es igual, imprimir que el número es un entero; de lo contrario, imprimir que no es un entero.

ALGORITMO

```
# Solicitar al usuario que ingrese un número

numero = float(input("Ingrese un número: “) )

# Verificar si el número es igual a su parte entera

if numero == int(numero):

        print(f"{numero} es un número entero.")

else:

        print(f"{numero} no es un número entero.")
```

```
01100010 01101001 01101110 01100001 01110010
01111001 00100000 01100011 01101111 01100100
01100101 00100000 01101001 01110011 00100000
01110100 01101000 01100101 00100000 01101100
01100001 01101110 01100111 01110101 01100001
01100111 01100101 00100000 01110101 01110011
01100101 01100100 00100000 01100010 01111001
00100000 01101101 01100001 01100011 01101000
01101001 01101110 01100101 01110011
```

ALGORITMO

Recomendación CM/Rec(2020)1 del Comité de Ministros del Consejo de Europa sobre el impacto en los Derechos Humanos de los sistemas algorítmicos, adoptada en la 1373ª reunión anual de 8 de abril de 2020

Sistemas algorítmicos

aplicaciones que, a menudo utilizando técnicas de optimización matemática, desarrollan una o más tareas como recopilar, combinar, limpiar, ordenar, clasificar e inferir datos, así como la selección, priorización, la elaboración de recomendaciones y toma de decisiones. Basándose en uno o más algoritmos para cumplir con sus requisitos en los entornos en los que se aplican, los sistemas algorítmicos automatizan las actividades de una manera que permiten la creación de servicios adaptables a escala y en tiempo real.

SISTEMA DE IA

Reglamento IA

«sistema de IA»: un sistema basado en una **máquina** que está diseñado para **funcionar con distintos niveles de autonomía** y que puede mostrar **capacidad de adaptación** tras el despliegue, y que, para objetivos explícitos o implícitos, **infiere de la información de entrada que recibe la manera de generar resultados de salida**, como predicciones, contenidos, recomendaciones o decisiones, que pueden influir en entornos físicos o virtuales;

Convención Marco CdE

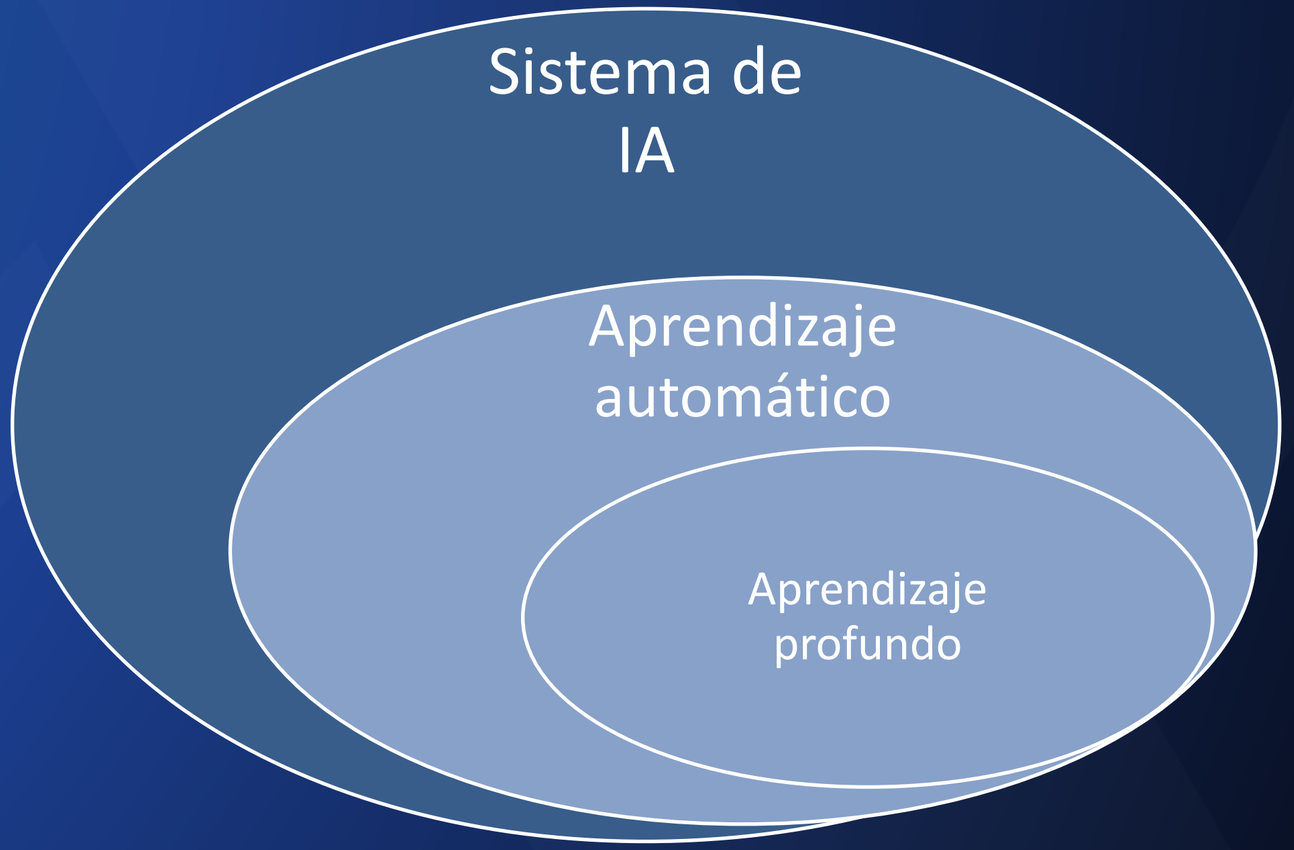
«sistema de inteligencia artificial» un sistema basado en **máquinas** que, con objetivos explícitos o implícitos**, infiere, a partir de los datos que recibe, cómo generar resultados**, como predicciones, contenidos, recomendaciones o decisiones que puedan influir en entornos físicos o virtuales. Los diferentes sistemas de inteligencia artificial varían en sus **niveles de autonomía y adaptabilidad** después de la implementación.

RD 817/2023

«Sistema de inteligencia artificial»: sistema diseñado para funcionar con un cierto nivel de **autonomía** y que, **basándose en datos de entradas** proporcionadas por máquinas o por personas, **infiere cómo lograr un conjunto de objetivos** establecidos utilizando estrategias de aprendizaje automático o basadas en la lógica y el conocimiento, y genera información de salida, como contenidos (sistemas de inteligencia artificial generativos), predicciones, recomendaciones o decisiones, que influyan en los entornos con los que interactúa.

SISTEMA DE IA

- Programa de ordenador, sólo o combinado con un dispositivo físico
- Autonomía para inferior cómo alcanzar el objetivo
- Utilización de estrategias de aprendizaje automático o estrategias basadas en la lógica y el conocimiento
- Producción de información de salida que influyen en los entornos con los que interactúa



Los sistemas que utilizan reglas definidas únicamente por personas físicas para ejecutar operaciones de manera automática no deben considerarse sistemas de IA.

DATOS PERSONALES

«datos personales»

toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona;

«categorías especiales de datos personales»

datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientación sexuales de una persona física

«datos genéticos»

datos personales relativos a las características genéticas heredadas o adquiridas de una persona física que proporcionen una información única sobre la fisiología o la salud de esa persona, obtenidos en particular del análisis de una muestra biológica de tal persona;

«datos relativos a la salud»

datos personales relativos a la salud física o mental de una persona física, incluida la prestación de servicios de atención sanitaria, que revelen información sobre su estado de salud;

«datos biométricos»

datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos;

«seudonimización»

el tratamiento de datos personales de manera tal que ya no puedan atribuirse a un interesado sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable;

TRATAMIENTO

cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción;

PERFILADO

toda forma de tratamiento automatizado de datos personales consistente en utilizar datos personales para evaluar determinados aspectos personales de una persona física, en particular para analizar o predecir aspectos relativos al rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación o movimientos de dicha persona física;

- debe ser una forma automatizada de tratamiento
- debe llevarse a cabo respecto a datos personales
- el objetivo de la elaboración de perfiles debe ser evaluar aspectos personales sobre una persona física

PERFILADO

toda forma de tratamiento automatizado de datos personales consistente en utilizar datos personales para evaluar determinados aspectos personales de una persona física, en particular para analizar o predecir aspectos relativos al rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación o movimientos de dicha persona física;

Recogida de datos

Análisis **automatizado** para identificar correlaciones

Aplicación de la correlación a una persona para analizar o predecir comportamientos

Artículo 22 RGPD

1. Todo interesado tendrá 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.

2. El apartado 1 no se aplicará si la decisión:

a) es necesaria para la celebración o la ejecución de un contrato entre el interesado y un responsable del tratamiento;

b) está autorizada por el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento y que establezca asimismo medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado, o

c) se basa en el consentimiento explícito del interesado.

3. En los casos a que se refiere el apartado 2, letras a) y c), el responsable del tratamiento adoptará las medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado, como mínimo el derecho a obtener intervención humana por parte del responsable, a expresar su punto de vista y a impugnar la decisión.

4. Las decisiones a que se refiere el apartado 2 no se basarán en las categorías especiales de datos personales contempladas en el artículo 9, apartado 1, salvo que se aplique el artículo 9, apartado 2, letra a) o g), y se hayan tomado medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado.

Artículo 22 RGPD

Elaboración de perfiles

≠

decisiones basadas únicamente en el tratamiento automatizado

Decisiones basadas únicamente en tratamientos automatizados

- Decisión basada **únicamente** en el tratamiento automatizado
- Que produzca **efectos jurídicos o significativamente similares**

NORMATIVA INTERNA

- Art. 23 de la Ley 15/2022, de 12 de julio, integral para la igualdad de trato y la no discriminación

- Disposición Adicional centésimo trigésima de la Ley 22/2021, de 28 de diciembre

- Disposición Adicional séptima de la Ley 28/2022, de 21 de diciembre, de fomento del ecosistema de las empresas emergentes

- Real Decreto 729/2023, de 22 de agosto, por el que se aprueba el Estatuto de la Agencia Española de Supervisión de Inteligencia Artificial

- Real Decreto 817/2023, de 8 de noviembre, que establece un entorno controlado de pruebas para el ensayo del cumplimiento de la propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial

NORMATIVA INTERNA

- Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público

- Real Decreto 203/2021, de 30 de marzo, por el que se aprueba el Reglamento de actuación y funcionamiento del sector público por medios electrónicos

- Sección 4ª del Capítulo I del Título III de la Ley 58/2003, de 17 de diciembre, General Tributaria

- Sección 3ª del Capítulo II del Título III del Real Decreto 1065/2007, de 27 de julio, por el que se aprueba el Reglamento General de las actuaciones y los procedimientos de gestión e inspección tributaria y de desarrollo de las normas comunes de los procedimientos de aplicación de los tributos

- Normativa de protección de datos personales: LO 3/2018 y LO 7/2021

NORMATIVA INTERNACIONAL

- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (RGPD)

- Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial (Reglamento de Inteligencia Artificial)

- Decisión de la Comisión, de 24 de enero de 2024, por la que se crea la Oficina Europea de Inteligencia Artificial

- Convención Marco del Consejo de Europa sobre Inteligencia Artificial y Derechos Humanos Derechos Humanos, Democracia y Estado de Derecho

SOFT LAW

- Carta de Derechos Digitales del Gobierno de España
- Código ético de la Inteligencia Artificial de la AEAT
- Guía de la AEPD de Adecuación al RGPD de tratamientos que incorporan Inteligencia Artificial
- Guía de la AEPD de Requisitos para Auditorías de Tratamientos que incluyan IA
- Directrices del EDPB sobre decisiones individuales automatizadas y elaboración de perfiles a los efectos del Reglamento 2016/679.

JURISPRUDENCIA

- Sentencia de la Sala de lo Contencioso de la Audiencia Nacional – Sección 7 2013/2024 - ECLI:ES:AN:2024:2013 de 30 de abril “sistema de información BOSCO”

- DICTAMEN 1/15 DEL TRIBUNAL DE JUSTICIA (Gran Sala) de 26 de julio de 2017 “Acuerdo PNR Canadá – UE”

- Sentencia del Tribunal Constitucional de la República Eslovaca de 10 de noviembre de 2021 (PL. ÚS 25/2019-117) “sistema e-kasa”

- Sentencia del Tribunal de Distrito de La Haya C/09/550982/HA ZA 18/388 de 5 de febrero de 2020 “SyRI”

- Sentencia del Consejo Constitucional Francia N° 2019-796 DC de 27 de diciembre de 2019

LA PROTECCIÓN DE DATOS COMO DERECHO FUNDAMENTAL

El derecho a la autodeterminación informativa

Art. 18.4 Constitución española

Art. 8 Carta DDFF UE

Convenio 108+ CdE para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal

PRINCIPIOS FUNDAMENTALES RGPD

- Licitud, lealtad y transparencia.
- Limitación de la finalidad.
- Minimización de datos.
- Exactitud.
- Limitación del plazo de conservación.
- Integridad y confidencialidad.
- Responsabilidad proactiva

Derechos de los ciudadanos:

- derecho de acceso,
- rectificación,
- supresión (derecho al olvido),
- limitación del tratamiento,
- portabilidad,
- oposición y
- no ser sometido a decisiones automatizdas

SUJETOS RESPONSABLES DE UN SISTEMA IA

RGPD

«responsable del tratamiento» o «responsable»: la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento;

«encargado del tratamiento» o «encargado»: la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento;

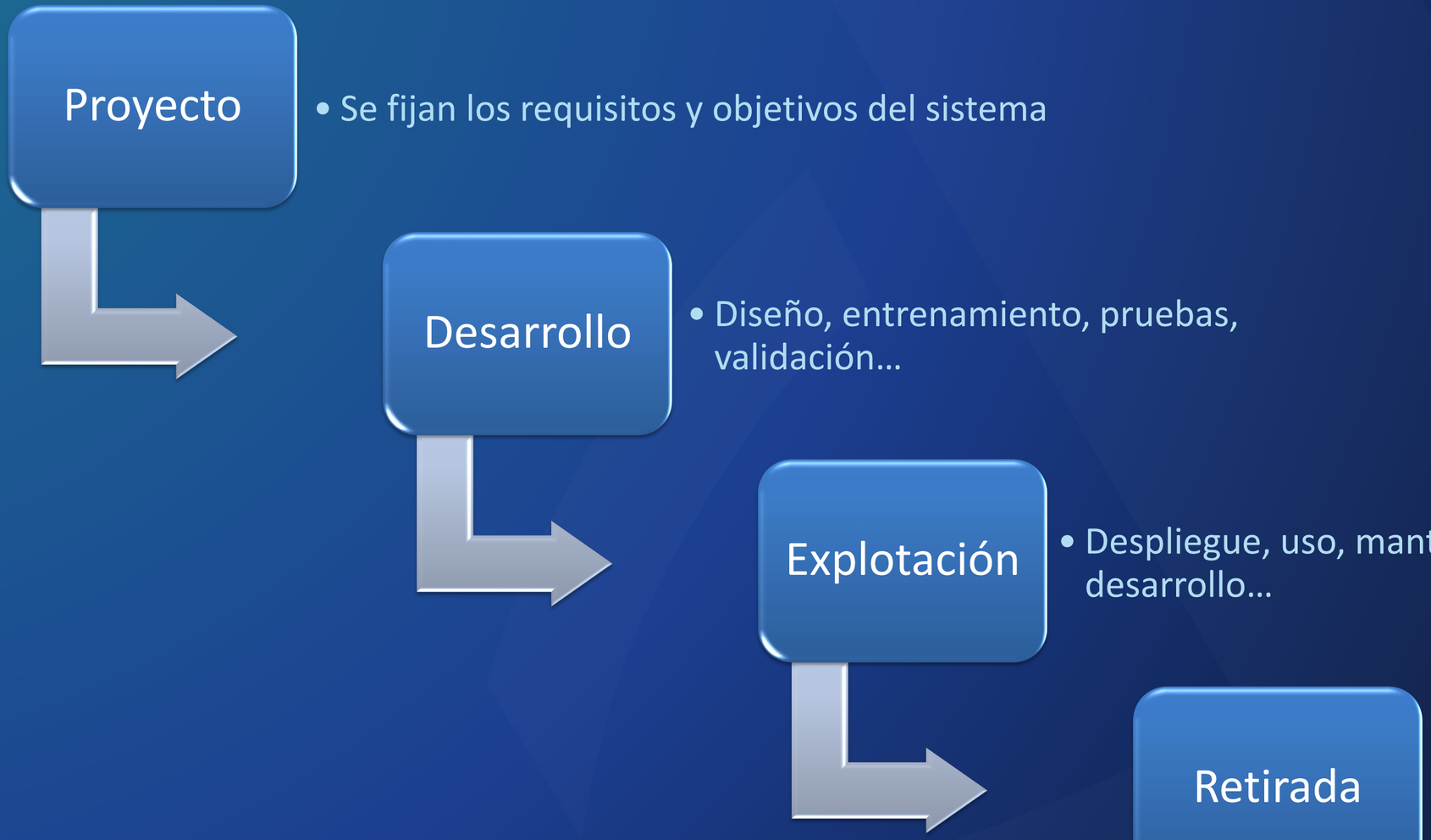
RIA

«operador»: un proveedor, fabricante del producto, responsable del despliegue, representante autorizado, importador o distribuidor

«responsable del despliegue»: una persona física o jurídica, o autoridad pública, órgano u organismo que utilice un sistema de IA bajo su propia autoridad, salvo cuando su uso se enmarque en una actividad personal de carácter no profesional

«proveedor»: una persona física o jurídica, autoridad pública, órgano u organismo que desarrolle un sistema de IA o un modelo de IA de uso general o para el que se desarrolle un sistema de IA o un modelo de IA de uso general y lo introduzca en el mercado o ponga en servicio el sistema de IA con su propio nombre o marca, previo pago o gratuitamente;

CICLO DE VIDA DE UN SISTEMA IA



Prohibidos

Permitidos sujetos a requisites y evaluación previa de conformidad

Permitidos sujetos a obligaciones de transparencia

Permitidos sin restricciones

SISTEMAS IA PROHIBIDOS (art. 5)

que se sirva de técnicas subliminales con el objetivo o el efecto de alterar de manera sustancial el comportamiento de una persona o un colectivo de personas

que explote alguna de las vulnerabilidades de una persona física o colectivo derivadas de su edad o discapacidad, o de una situación social o económica específica, con la finalidad o el efecto de alterar de manera sustancial el comportamiento

para evaluar o clasificar a personas físicas o a colectivos atendiendo a su comportamiento social o a características personales o de su personalidad conocidas, inferidas o predichas, de forma que la puntuación ciudadana resultante provoque:

i) un trato perjudicial o desfavorable en contextos sociales que no guarden relación con los contextos donde se generaron o recabaron los datos originalmente,

ii) un trato perjudicial o desfavorable que sea injustificado o desproporcionado con respecto a su comportamiento social o la gravedad de este;

para realizar evaluaciones de riesgos de personas físicas con el fin de valorar o predecir el riesgo de que una persona física cometa un delito basándose únicamente en la elaboración del perfil de una persona física o en la evaluación de los rasgos y características de su personalidad

que creen o amplíen bases de datos de reconocimiento facial mediante la extracción no selectiva de imágenes faciales de internet o de circuitos cerrados de televisión

para inferir las emociones de una persona física en los lugares de trabajo y en los centros educativos

sistemas de categorización biométrica que clasifiquen individualmente a las personas físicas sobre la base de sus datos biométricos para deducir o inferir su raza, opiniones políticas, afiliación sindical, convicciones religiosas o filosóficas, vida sexual u orientación sexual

sistemas de identificación biométrica remota «en tiempo real» en espacios de acceso público con fines de garantía del cumplimiento del Derecho, con excepciones

SISTEMAS IA ALTO RIESGO

Destinado a ser utilizado como componente de seguridad de un producto en el ámbito de las normas enumeradas en ANEXO I

Obligación de registro base datos UE

Contemplados en el anexo III salvo que no plantee un riesgo importante de causar un perjuicio a la salud, la seguridad o los derechos fundamentales de las personas físicas, también al no influir sustancialmente en el resultado de la toma de decisiones:

- que el sistema de IA esté destinado a realizar una tarea de procedimiento limitada;
- que el sistema de IA esté destinado a mejorar el resultado de una actividad humana previamente realizada;
- que el sistema de IA esté destinado a detectar patrones de toma de decisiones o desviaciones con respecto a patrones de toma de decisiones anteriores y no esté destinado a sustituir la valoración humana previamente realizada sin una revisión humana adecuada, ni a influir en ella, o
- que el sistema de IA esté destinado a realizar una tarea preparatoria para una evaluación que sea pertinente

los sistemas de IA a que se refiere el anexo III siempre que efectúe la elaboración de perfiles de personas físicas.

(59)… **Los sistemas de IA destinados específicamente a ser utilizados en procesos administrativos por las autoridades fiscales y aduaneras** y las unidades de inteligencia financiera que desempeñan tareas administrativas de análisis de información de conformidad con el Derecho de la Unión en materia de lucha contra el blanqueo de capitales **no deben clasificarse como sistemas de IA de alto riesgo usados por las autoridades garantes del cumplimiento del Derecho con el fin de prevenir, detectar, investigar y enjuiciar delitos.**

Requisitos sistemas IA Alto Riesgo

Se contará con un sistema de gestión de riesgos

Se establecerá una gobernanza y gestión de los datos de entrenamiento y prueba, asegurando buenas prácticas en su diseño, recolección y preparación, asegurando su relevancia y corrección y sus apropiadas propiedades estadísticas, evitando sesgos que afecten negativamente a las personas

Irán acompañados de documentación técnica actualizada, que demuestre que se cumplen los requisitos exigidos

Tomarán automáticamente registros de actividad del sistema (‘logs’)

Se aportará información a los usuarios sobre las capacidades del sistema, sus requisitos de equipamiento, su ámbito de aplicación, su nivel de precisión, las condiciones de utilización que pueden implicar riesgos, los sistemas para supervisión humana, etc.

Se diseñarán y desarrollarán de modo que puedan ser vigilados de manera efectiva por personas físicas durante el período que estén en uso

Proporcionaran un nivel adecuado de precisión, solidez y ciberseguridad

Obligaciones de los responsables del despliegue de sistemas de IA de alto riesgo

- Adoptarán medidas técnicas y organizativas adecuadas para garantizar que utilizan dichos sistemas con arreglo a las instrucciones de uso que los acompañen
- Encomendarán la supervisión humana a personas físicas que tengan la competencia, la formación y la autoridad necesarias
- Asegurará que los datos de entrada sean pertinentes y suficientemente representativos en vista de la finalidad prevista del sistema de IA de alto riesgo, en la medida en que ejerza el control sobre dichos datos
- Vigilarán el funcionamiento del sistema de IA de alto riesgo basándose en las instrucciones de uso y, cuando proceda, informarán a los proveedores y autoridades de control
- Conservarán, al menos 6 meses, los ‘logs’ que los sistemas de IA de alto riesgo generen automáticamente
- Cuando sean empleadores informarán a los representantes de los trabajadores y a los trabajadores afectados de que estarán expuestos a la utilización del sistema de IA de alto riesgo
- Cuando proceda realizará una evaluación de impacto del RGPD
- Cuando sean autoridades públicas, antes de ponerlo en servicio se registrarán, seleccionarán el sistema y registrarán su utilización en la base de datos de la UE
- Cuando el sistema tome decisiones o ayude a tomar decisiones relacionadas con personas físicas las informarán de que están expuestas a la utilización de los sistemas de IA de alto riesgo
- Autorización judicial o administrativa al uso de sistemas de identificación biométrica remota para la búsqueda selectiva de una persona sospechosa de haber cometido un delito o condenada por ello
- Cooperarán con las autoridades competentes pertinentes en cualquier medida que estas adopten en relación con el sistema de IA de alto riesgo
- En determinados casos (art. 27) realizar una evaluación de impactorelativa a los derechos fundamentales

Evaluación de impacto relativa a los derechos fundamentales

OBJETO: Sistemas de alto riesgo organismos de Derecho público Anexo III salvo infraestructuras críticas

¿CUÁNDO? al primer uso y cuando se modifiquen los elementos analizados

¿QUÉ?

a) una descripción de los procesos en los que se utilizará el sistema de IA de alto riesgo;

b) una descripción del período de tiempo durante el cual se prevé utilizar cada sistema de IA de alto riesgo y la frecuencia con la que está previsto utilizarlo;

c) las categorías de personas físicas y colectivos que puedan verse afectados por su utilización en el contexto específico;

d) los riesgos de perjuicio específicos que puedan afectar a las categorías de personas físicas y colectivos determinadas;

e) una descripción de la aplicación de medidas de supervisión humana, de acuerdo con las instrucciones de uso;

f) las medidas que deben adoptarse en caso de que dichos riesgos se materialicen, incluidos los acuerdos de gobernanza interna y los mecanismos de reclamación.

Sistemas sujetos a obligaciones de transparencia

SISTEMA DE RECONOCIMIENTO DE EMOCIONES O CATEGORIZACIÓN BIOMÉTRICA: informarán del funcionamiento del sistema a las personas físicas expuestas a él y tratarán sus datos personales de conformidad con los Reglamentos (UE) 2016/679 y (UE) 2018/1725 y con la Directiva (UE) 2016/680 salvo que hayan sido autorizados por ley con sujeción a las garantías adecuadas para los derechos y libertades de terceros

SISTEMA DE IA QUE GENERE O MANIPULE IMÁGENES O CONTENIDOS DE AUDIO O VÍDEO QUE CONSTITUYAN UNA ULTRASUPLANTACIÓN: harán público que estos contenidos o imágenes han sido generados o manipulados de manera artificial salvo cuando la ley autorice su uso para para detectar, prevenir, investigar o enjuiciar delitos

SISTEMA DE IA QUE GENERE O MANIPULE TEXTO QUE SE PUBLIQUE CON EL FIN DE INFORMAR AL PÚBLICO SOBRE ASUNTOS DE INTERÉS PÚBLICO: divulgarán que el texto se ha generado o manipulado de manera artificial salvo cuando el uso esté autorizado por ley para detectar, prevenir, investigar o enjuiciar delitos, o cuando el contenido generado por IA haya sido sometido a un proceso de revisión humana o de control editorial y cuando una persona física o jurídica tenga la responsabilidad editorial por la publicación del contenido.

SISTEMAS DE IA DESTINADOS A INTERACTUAR DIRECTAMENTE CON PERSONAS FÍSICAS: los proveedores garantizarán que se diseñen y desarrollen de forma que las personas físicas de que se trate estén informadas de que están interactuando con un sistema de IA, excepto cuando resulte evidente desde el punto de vista de una persona física razonablemente informada, atenta y perspicaz, teniendo en cuenta las circunstancias y el contexto de utilización

PRINCIPIO DE TRANSPARENCIA

el responsable del tratamiento facilitará al interesado información sobre la existencia de decisiones automatizas, incluida la elaboración de perfiles, a que se refiere el artículo 22, apartados 1 y 4, y, al menos en tales casos, información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado

- ✓Datos de entrada utilizados y su antigüedad
- ✓Importancia relativa de los datos en la toma de decisión
- ✓Calidad de los datos de entrenamiento y patrones utilizados
- ✓Valores de precisión/error del sistema
- ✓Existencia o no de supervisión humana cualificada
- ✓Referencia a auditorías o certificaciones del sistema IA

LA GESTIÓN DE RIESGOS
EIPD

Art 35 RGPD

Cuando sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento realizará, antes del tratamiento, una evaluación del impacto de las operaciones de tratamiento en la protección de datos personales.

– Art 28 LOPD

a) Cuando el tratamiento pudiera generar situaciones de discriminación, usurpación de identidad o fraude, pérdidas financieras, daño para la reputación, pérdida de confidencialidad de datos sujetos al secreto profesional, reversión no autorizada de la seudonimización o cualquier otro perjuicio económico, moral o social significativo para los afectados.

…

d) Cuando el tratamiento implicase una evaluación de aspectos personales de los afectados con el fin de crear o utilizar perfiles personales de los mismos, en particular mediante el análisis o la predicción de aspectos referidos a su rendimiento en el trabajo, su situación económica, su salud, sus preferencias o intereses personales, su fiabilidad o comportamiento, su solvencia financiera, su localización o sus movimientos.

…

f) Cuando se produzca un tratamiento masivo que implique a un gran número de afectados o conlleve la recogida de una gran cantidad de datos personales.

…

h) Cualesquiera otros que a juicio del responsable o del encargado pudieran tener relevancia y en particular aquellos previstos en códigos de conducta y estándares definidos por esquemas de certificación.

MEDIDAS PARA LA GESTIÓN DE RIESGOS

- Minimizar la cantidad de datos que son tratados.
- Agregar los datos personales en la medida de lo posible.
- Ocultar los datos personales y sus interrelaciones para limitar su exposición y que no sean visibles por partes no interesadas.
- Separar los contextos de tratamiento para dificultar la correlación de fuentes de información independientes, así como la posibilidad de inferir información.
- Mejorar la Información a los interesados.
- Proporcionar medios a interesados para que puedan controlar sus datos.
- Documentar para demostrar, el cumplimiento de la política de protección de datos.

GOBERNANZA DE LOS DATOS: CALIDAD Y MINIMIZACIÓN

Factores que influyen en la exactitud

La propia implementación del sistema IA (errores de hardware, programación…

El conjunto de datos de entrenamiento o validación está viciado con errores, información deliberadamente errónea o sesgos (mala calidad de los datos, datos ausentes, o muestreo selectiva, errores de representación y medida)

La evolución sesgada del modelo IA (sesgos de realimentación)

GOBERNANZA DE LOS DATOS: CALIDAD Y MINIMIZACIÓN

Técnicas de minimización de datos

Análisis previo de las condiciones que han de cumplir los datos para la aplicación concreta.
Análisis de la tipología de datos empleados en cada etapa del sistema IA.
Supresión de datos no estructurados, o información no necesaria recogida durante el preproceso de la información.
Identificación y supresión, durante el proceso de entrenamiento, aquellas categorías de datos que no tienen una influencia significativa en el aprendizaje o en el resultado de la inferencia.
Supresión de conclusiones no relevantes asociadas a información personal durante el proceso de entrenamiento.
Utilización de técnicas de verificación y modelos de aprendizaje que requieran un menor número de datos.
Entrenamiento con datos cifrados.
Agregación de datos.
Anonimización y seudonimización, también en los datos de entrenamiento.

XVIII
Derechos digitales de la ciudadanía en sus relaciones con las Administraciones Públicas

6. Se promoverán los derechos de la ciudadanía en relación con la inteligencia artificial reconocidos en esta Carta en el marco de la actuación administrativa reconociéndose en todo caso los derechos a:

a) Que las decisiones y actividades en el entorno digital respeten los principios de buen gobierno y el derecho a una buena Administración digital, así como los principios éticos que guían el diseño y los usos de la inteligencia artificial.
b) La transparencia sobre el uso de instrumentos de inteligencia artificial y sobre su funcionamiento y alcance en cada procedimiento concreto y, en particular, acerca de los datos utilizados, su margen de error, su ámbito de aplicación y su carácter decisorio o no decisorio.
La ley podrá regular las condiciones de transparencia y el acceso al código fuente, especialmente con objeto de verificar que no produce resultados discriminatorios.

c) Obtener una motivación comprensible en lenguaje natural de las decisiones que se adopten en el entorno digital, con justificación de las normas jurídicas relevantes, tecnología empleada, así como de los criterios de aplicación de las mismas al caso. El interesado tendrá derecho a que se motive o se explique la decisión administrativa cuando esta se separe del criterio propuesto por un sistema automatizado o inteligente.
d) Que la adopción de decisiones discrecionales quede reservada a personas, salvo que normativamente se prevea la adopción de decisiones automatizadas con garantías adecuadas.

7. Será necesaria una evaluación de impacto en los derechos digitales en el diseño de los algoritmos en el caso de adopción de decisiones automatizadas o semiautomatizadas.

XXV
Derechos ante la inteligencia artificial

La inteligencia artificial deberá asegurar un enfoque centrado en la persona y su inalienable dignidad, perseguirá el bien común y asegurará cumplir con el principio de no maleficencia.

2. En el desarrollo y ciclo de vida de los sistemas de inteligencia artificial:

Se deberá garantizar el derecho a la no discriminación cualquiera que fuera su origen, causa o naturaleza, en relación con las decisiones, uso de datos y procesos basados en inteligencia artificial.
Se establecerán condiciones de transparencia, auditabilidad, explicabilidad, trazabilidad, supervisión humana y gobernanza. En todo caso, la información facilitada deberá ser accesible y comprensible.
Deberán garantizarse la accesibilidad, usabilidad y fiabilidad.

3. Las personas tienen derecho a solicitar una supervisión e intervención humana y a impugnar las decisiones automatizadas tomadas por sistemas de inteligencia artificial que produzcan efectos en su esfera personal y patrimonial.

CÓDIGO ÉTICO AEAT

PRINCIPIOS ÉTICOS

1. Centralidad humana.
2. Legalidad.
3. Transparencia.
4. Equidad.
5. Calidad.

Sentencia de la Sala de lo Contencioso de la Audiencia Nacional – Sección 7 2013/2024 - ECLI:ES:AN:2024:2013 de 30 de abril “sistema de información BOSCO”

Un algoritmo es el que decide quién recibe el bono social para la luz. El Gobierno y los jueces se niegan a enseñar el código

- La organización pro-transparencia Civio recibe el rechazo de la Audiencia Nacional en su intento de conocer el código fuente del sistema BOSCO
- La Justicia española vuelve a ofrecer pobres argumentos técnicos
- El Gobierno defiende la transparencia algorítmica, pero luego mira hacia otro lado

DICTAMEN 1/15 DEL TRIBUNAL DE JUSTICIA (Gran Sala) de 26 de julio de 2017 “Acuerdo PNR Canadá – UE”

No se tomarán «decisiones que afecten gravemente a un [pasajero] únicamente en razón del tratamiento automático de los datos del [PNR]».

Los modelos y criterios preestablecidos de riesgo utilizados para seleccionar personas por procedimientos automatizados deben:

(1) Basarse en bases de datos fiables, actualizadas y directamente vinculadas al objetivo del análisis de riesgos

(2) Que no entrañen (directa o indirectamente) riesgo de discriminación; y

(3) los modelos y criterios preestablecidos deben ser específicos y fiables, de modo que permitan llegara resultados que seleccionen individuos sobre los que podría recaer una «sospecha razonable»

Sentencia del Tribunal de Distrito de La Haya C/09/550982/HA ZA 18/388 de 5 de febrero de 2020 “SyRI”

Legislación SyRI infringe:

- **Necesidad de EIPD por cada proyecto de investigación**
- **Principio de transparencia**
  - **no proporciona información sobre qué datos fácticos objetivos pueden llevar justificadamente a la conclusión de que existe un riesgo aumentado**
  - **no proporciona información sobre el funcionamiento del modelo de riesgos, por ejemplo, el tipo de algoritmos utilizados en el modelo, ni proporciona información sobre el método de análisis de riesgos aplicado**
- **Principio de minimización**
- **Prohibición de discriminación**

La Administración Financiera ha introducido un proyecto de conexión en línea de todas las cajas registradoras al portal de la Administración Financiera - eKasa. Forma parte de las medidas de lucha contra el fraude fiscal. Desde 2012, ya hemos implementado decenas de medidas de planes de acción para combatir el fraude fiscal (por ejemplo, cobra fiscal, declaración de control del IVA o limitación de pagos en efectivo). **Gracias a ellos, redujimos la brecha fiscal del 41% al 26% y aportamos 3.700 millones de euros más al erario público.**

Sin embargo, la cuantía de la brecha del IVA en los sectores HORECA (hoteles, restaurantes, cafeterías), comercio minorista y servicios sigue siendo elevada. Solo en 2014 ascendió a 491 millones de euros. Por lo tanto, a fin de luchar contra el fraude fiscal, es necesario adoptar nuevas medidas para eliminarlo. Desde la introducción de eKasa, la Administración Financiera espera reducir la brecha del IVA en estos sectores.

Mientras que hasta ahora los empresarios tenían la oportunidad de elegir una conexión a los sistemas de administración financiera (en forma de VCR) de forma voluntaria, ahora la conexión online a la administración financiera es obligatoria. eKasa es una solución en línea moderna con importantes beneficios para los emprendedores.

Las cajas registradoras electrónicas (ERP) se han convertido en cajas registradoras en línea (ORP). Sin embargo, los emprendedores han ampliado las posibilidades: la caja registradora puede ser no solo un ERP clásico, sino también una tableta, un móvil, un ordenador o una videograbadora. A partir del 1 de abril de 2019, todas las operaciones de nueva creación y las nuevas cajas registradoras (aquellas que comenzaron a registrar ventas después del 1.4.) tuvieron que unirse al sistema, todas las demás entidades gradualmente hasta el 30 de junio de 2019. A partir del 1 de julio de 2019, todos los emprendedores deben estar conectados al sistema eKasa en todos los ámbitos.

https://www.financnasprava.sk/sk/podnikatelia/dane/ekasa

Sentencia del Tribunal Constitucional de la República Eslovaca de 10 de noviembre de 2021 (PL. ÚS 25/2019-117) “sistema e-kasa”

(i) transparencia, debe informarse a la persona afectada de que la actuación de la autoridad pública, como su decisión, se ve influido por el uso de un sistema automatizado, siendo informado de la existencia, el alcance y las implicaciones de la evaluación de su persona por medios automatizados, ya sea a través de registros públicos, instrucciones específicas o de otro tipo;

(ii) medidas de protección individual eficientes y accesibles y confiadas a autoridades de supervisión independientes; y

(iii) mecanismos de supervisión que funcionen tanto ex ante (antes del despliegue) como ex post (posterior al despliegue) para evaluar la calidad del sistema, sus componentes, los porcentajes de error y las imperfecciones.

Sentencia del Consejo Constitucional Francia N° 2019-796 DC de 27 de diciembre de 2019

art. 154 de la LEY nº 2019-1479, de 28 de diciembre de 2019, sobre finanzas para 2020 contemplaba una habilitación experimental a las autoridades tributarias y aduaneras francesas para recoger y utilizar de forma automatizada contenidos accesibles al público en los sitios web de determinados operadores de plataformas, con el fin de investigar infracciones e infracciones en materia fiscal y aduanera.

1. los datos que pueden recogerse y utilizarse deben cumplir dos requisitos acumulativos: (i) ser un contenido de libre acceso en un servicio de comunicación pública en línea y (ii) ser claramente hechos públicos por los usuarios de dichos sitios.
2. se excluyen expresamente los datos sensibles, no pudiendo incluir ningún sistema de reconocimiento facial.
3. sólo podrán ser utilizados por funcionarios de las autoridades fiscales y aduaneras con determinado nivel de responsabilidad
4. sólo el diseño de las herramientas de tratamiento de datos, excluyendo su recogida, tratamiento y almacenamiento, puede confiarse a un subcontratista de la Administración
5. las personas que intervienen en el diseño y en la ejecución de las operaciones de tratamiento de que se trata están sujetas al secreto profesional
6. los datos manifiestamente ajenos a las infracciones y violaciones solicitadas o que constituyan datos sensibles deben destruirse a más tardar en un plazo de cinco días a partir de su recogida, sin que se vuelva a utilizar dichos datos durante ese período. Los demás datos deberán destruirse en un plazo de treinta días si no son tales que contribuyan a la determinación de infracciones. Solo podrán conservarse los datos estrictamente necesarios para tal determinación, en el plazo de un año o, en su caso, hasta el final de los procedimientos penales, fiscales o aduaneros en cuyo contexto se utilicen.
7. cuando el tratamiento efectuado permita acreditar la existencia de indicios de que una persona puede haber cometido alguna de las infracciones perseguidas, los datos recogidos se transmitirán al servicio competente de la administración para su corroboración y análisis, de modo que no puede incoarse ningún procedimiento penal, fiscal o aduanero sin una apreciación individual de la situación de la persona por parte de la Administración, que se base exclusivamente en los resultados del tratamiento automatizado.
8. contempla expresamente el ejercicio del derecho de acceso a los datos, por las personas interesadas.

MUCHAS GRACIAS

Agencia Tributaria