UNIVERSIDAD INTERNACIONAL DE LA RIOJA unir

Ética y legalidad en aplicaciones basadas en inteligencia artificial

Federico Damián Estebanez

Introducción

En abril de 2016, el Parlamento Europeo adopta por primera vez a nivel europeo la regulación de la protección de datos generales.

Con ella se persigue de normalizar el manejo de datos personales. Esto normalizará las aplicaciones de inteligencias artificial.

Ética y legalidad en aplicaciones basadas en inteligencia artificial

Debido al peligro para la privacidad individual y de la sociedad que puede suponer el uso sin orden de los datos, ha sido necesario marcar normas estrictas en su recogida.

Los proyectos de inteligencia artificial están basados en estos datos.
Sin ellos y su análisis, esta disciplina no es posible.

Por ello, esta ciencia se encuentra fuertemente influenciada por dicha legislación.

Nacionalmente, el órgano encargado de poner orden en el asunto es la Agencia Española de Protección de Datos (AEPD), quién aprobó la Ley Orgánica de Protección de Datos de Carácter Personal (LOPD) 15/1999.

Esta se ha visto recientemente regulada bajo el mando Unión Europea, mediante el Reglamento General de Protección de Datos (RGPD).

Entró en vigor el 25 de mayo de 2016, pasando a ser su cumplimento obligatorio una vez transcurridos 2 años desde la fecha, de forma que las empresas tuvieron tiempo suficiente para ajustarse.

Los aspectos más destacados de este reglamento son las siguientes.

1. Protección de datos de carácter personal

La legislación protege los datos que distinguen directamente a una persona, como el DNI. No obstante, también los que pueden hacerlo de forma indirecta por cruce de datos.

Esto no conlleva que el almacenamiento de información personal esté totalmente prohibido, ya que si así lo fuese las empresas de institución pública no podrían funcionar. El objetivo es establecer una mayor seguridad, privacidad y control de ellos.

La LOPD, permite el uso de datos siempre que el usuario lo consienta. Los responsables de recopilar los datos deben garantizar la posibilidad de rectificación y cancelación de la información suministrada.

2. Confianza

Para que el usuario ceda sus datos debe de existir una confianza con el organismo, basado en los siguientes puntos.

- El usuario es consciente de la institución que usa los datos y para que los usa.
- El usuario conoce la causa del valor de sus datos.
- El usuario es asegurado de la seguridad en el tratamiento y privacidad de sus datos.

3. Anonimización de datos personales

Para garantizar los puntos 1 y 2, y a su vez obtener beneficios de los datos, es requerido anonimizar la información recogida. Para hacerse efectiva, juega un papel muy importante la irreversibilidad.

La anomización debe atender los siguientes principios:

1. Principio proactivo: Ante una fuga de información producida, se garantizará la privacidad de forma proactiva.

2. Principio de veracidad por defecto: Se debe considerar el grado de detalle que deben tener los datos anonimizados para garantizar la anomización en conjunto.

3. Principio de privacidad objetiva: Siempre existirá un mínimo riesgo de reidentificación de la información que deberá ser aceptada.

4. Principio de plena funcionalidad: El proceso de anomización debe garantizar la utilidad de los datos en base a los objetivos establecidos.

5. Principio de privacidad en el ciclo de vida de la información: Privacidad durante todo el proceso.

6. Principio de información y formación: Todo personal con acceso a los datos deben estar correctamente formados.

Para asegurar tales principios con su anonimización existen diferentes procedimientos:

a) Desnaturalizar: Transformar la naturaleza del dato, por ejemplo, clasificando la información por rangos.
b) Cifrar: Ilegibilizar los datos, mediante cifrado.
c) Tokenizar: Reemplazar el valor por otro dato sin relación.
d) Funciones hash: Aplicación de funciones matemáticas al dato.
e) Disociar: Eliminar parte de la información.

La aplicación de estos aspectos del reglamento es de obligado cumplimiento desde 2018, debido a la RGPD.

Su estricto cumplimiento supone un desafío para seguir sacando el máximo beneficio a los datos, sin caer en la infracción y por ende en grandes multas.

Éticamente, se estudia también:

- La discriminación resultante del análisis de datos.
- La interpretación interesada.
- La fiabilidad de los resultados.

El objetivo debe de ser de win-win para la sociedad, la compañía y los clientes, respetado los derechos fundamentales del ciudadano.

Esta regulación de los datos personales no impedirá el avance de la inteligencia artificial. Solo tratará de dirigirla a una buena causa.

No obstante, el debate de con qué grado de seguridad se cumple esta ley en las distintas empresas quedará abierto, al ser un tema tan oculto y difícil de investigar por los medios. Por ello, con el paso del tiempo las leyes pasarán a ser más restrictivas y las empresas deben de estar preparadas para ello.

Estos datos y su inteligencia son el camino al futuro. Ambos sujetos definirán la actividad humana y de las máquinas, dando lugar a grandes cambios en la economía.

Actualmente, la pregunta de si las maquinas aparte de llevar a cabo comportamientos inteligentes con dichos datos, serán capaces de pensar de forma similar a la humana, queda abierta. Si esto algún día llega a desarrollarse, no hay duda de que la ley se desarrollará de igual forma para continuar controlando la seguridad ciudadana.

Bibliografía

Goodman, B. &. (2016). Retrieved from European Union regulations on algorithmic decision-making and a «right to explanation»: https://arxiv.org/pdf/1606.08813.pdf

UNIR. (n.d.). Retrieved from Implicaciones filosóficas, éticas y legales en la aplicación de la inteligencia artificial: https://campusvirtual.unir.net/