Blog ECIJA 2.0

31 de Octubre de 2018

Elena Peña

abogado de ECIJA

¿Es la protección de datos una barrera en el desarrollo de la inteligencia artificial?

El pasado 23 de octubre se publicaron las Directrices Universales para la Inteligencia Artificial, que ponen de relieve la necesidad de encontrar un equilibrio entre este avance tecnológico y el derecho fundamental a la privacidad en el marco del RGPD.

Fue en 1997 cuando la inteligencia artificial pasó de un concepto que comúnmente se asociaba con películas de ciencia ficción futuristas a una realidad, cuando el campeón mundial de ajedrez Gary Kasparov cayó ante la supercomputadora de IBM Deep Blue.

Dos décadas después, los avances en este tipo de tecnología se han

vista no lo parezca, este avance supuso un salto estratosférico, ya que en vez de aprender únicamente de la información con la que se le alimentó, el programa se entrenó jugando contra sí mismo, llegando a desarrollar estrategias desconocidas hasta el momento. Es más, la siguiente versión, AlphaGo Zero, aprendió sin información sobre partidas anteriores: fue programado únicamente con las normas del juego, y tras 40 días jugando contra sí mismo ganó a la versión anterior del programa 100-0, requiriendo mucha menos energía.

Ahora, la **inteligencia artificial** va haciéndose un hueco en nuestro día a día: desde los avances en coches autónomos, a aplicaciones de música que hacen sugerencias en base a nuestro historial de reproducciones o *chatbots* en páginas web que nos ofrecen su ayuda.

En este escenario hay quien piensa que la entrada en aplicación del **Reglamento Europeo de Protección de Datos** (RGPD) supondrá un freno a estos avances tecnológicos cuando la información analizada contenga datos personales. Sin embargo, de cara a que el progreso de esta tecnología se construya de manera eficiente es necesario considerar la privacidad como la base en la que debe apoyarse, y no como el techo que frene su crecimiento.

La inteligencia artificial es en esencia una forma de explotar Big Data, siendo actualmente el llamado ***machine learning*** o aprendizaje automático su rama más comercializada. Esta técnica supone la creación de algoritmos matemáticos basados en el análisis de grandes cantidades de datos, extrayendo correlaciones para crear modelos que posteriormente se aplican a nueva información. Así, esta herramienta es capaz de aprender de su propia experiencia, incluso con independencia del aporte de información por parte del hombre.

Atendiendo a esta definición, podemos afirmar que los datos son la gasolina de la inteligencia artificial. De ahí que actualmente las empresas sientan rechazo a la hora de eliminar información, y tiendan a almacenar un abanico de datos de cada titular mayor del necesario, al considerar que en algún momento podrán sacarle rendimiento. Sin embargo, cuando se utilicen datos personales, esta consideración entra en conflicto con dos principios de la protección de datos: la **minimización de datos** y la **limitación de la finalidad**.

Así, de acuerdo al RGPD, únicamente podrán tratarse aquellos datos adecuados, pertinentes y limitados a lo necesario en relación con los fines, que a su vez deben ser determinados, explícitos y legítimos. Una excepción a esta prohibición de tratamiento ulterior con fines distintos sería en el caso de que la nueva finalidad fuera, entre otras, la de investigación científica. La cuestión a dirimir sería, ¿puede llegar a considerarse el desarrollo de herramientas de inteligencia artificial como subsumible en este concepto de "investigación científica"? Teniendo en cuenta que en el considerando 159 se indica que dicho concepto debe ser interpretado de manera amplia, esta decisión parece fácil en aquellos casos en que el objetivo sea, por ejemplo, la investigación de enfermedades, pero si el fin tiene un carácter comercial parece más complicado defender dicha postura, por lo que habrá que atender a cada caso.

interesado o le afecte de manera significativa, se añaden consideraciones al genérico deber de informar del tratamiento de datos. En estos casos, deberá trasladarse a su vez al interesado, entre otros, información relevante sobre la lógica implicada en la toma de decisiones. Esto puede suponer una complicación, ya que por la naturaleza de esta tecnología no siempre es posible determinar cómo se ha llegado a ese resultado o razonarlo en términos entendibles al ser humano. A este fenómeno se le conoce **Black Box** o caja negra: se desconoce el proceso seguido por el sistema a la hora de llegar a una conclusión, renunciando al porqué en pos del qué.

El Grupo de Trabajo del artículo 29 ha entendido que esta complejidad no es excusa suficiente para evitar cumplir con la obligación de informar, aunque interpretó de manera suavizada este requisito entendiendo que lo que se traslade al interesado debe ser suficientemente comprensible para que pueda entender las razones detrás de la decisión, pero sin necesidad de dar una explicación compleja sobre los algoritmos utilizados o revelar el algoritmo completo**[1]**.

La **exactitud** de los datos tratados mediante inteligencia artificial y sus conclusiones es también un punto de conflicto desde la óptica de la protección de datos, al tratarse de uno de los principios a cumplir según el RGPD (art. 5). Cuando los datos que se tratan no son representativos de la muestra, o la información obtenida es inexacta o errónea, se cumple la premisa de "*garbage in, garbage out*": si incluyes información inexacta o errónea, tus conclusiones lo serán a su vez. En la práctica esto puede derivar en situaciones de discriminación, como pudimos comprobar en el caso de Tay, el *chatbot* de Microsoft que aprendía de conversaciones de usuarios de Twitter, lo que supuso que sus contestaciones incluyeran comentarios racistas y sexistas, y fuera dado de baja a 24 horas después de su lanzamiento.

El espíritu del RGPD no es que estos posibles puntos de conflicto paralicen el desarrollo tecnológico, recogiendo a su vez medidas tendentes a que la protección de datos vaya de la mano de los avances tecnológicos en vez de ponerles freno. Por un lado, tenemos el principio de ***Privacy by Design,*** entendiéndose que desde el diseño de la tecnología se deberá tener en cuenta el concepto de privacidad. Otro de los efectos que tendrá a medio y largo plazo el RGPD será la tendencia a la **pseudonimización**, o en la medida de lo posible **anonimización**, de los datos personales. Asimismo, con frecuencia los tratamientos de datos en los que se utilicen herramientas de inteligencia artificial deberán ser objeto de una **evaluación de impacto o PIA** para analizar los efectos sobre los derechos y libertades de los interesados, al tratarse de tecnologías innovadoras e ir asociados normalmente a la elaboración de perfiles.

Por lo tanto, las implicaciones comentadas no deben entenderse como barreras, sino como la manera de equilibrar los avances en nombre de la inteligencia artificial y la privacidad, y lograr así un desarrollo que no suponga un reto para los derechos fundamentales.

---

[1] Guidelines on Automated individual decision-making and Profiling for