La IA en Europa: el difícil equilibrio entre regulación e innovación

Una conversación de Sampsa Samila con Gabriele Mazzini

1 de agosto de 2024

El Reglamento de Inteligencia Artificial de la Unión Europea, la primera ley del mundo en esta materia, se ha concebido para garantizar la seguridad, transparencia, trazabilidad y no discriminación de la innovación en IA. ¿Tendrá éxito? Su principal arquitecto explica los principios e implicaciones de esta

normativa.

Tras años de disputas políticas, el pasado mes de mayo el Consejo Europeo adoptó oficialmente el Reglamento de Inteligencia Artificial, cuyas obligaciones se aplicarán escalonadamente en los Estados miembros hasta su completa entrada en vigor a mediados de 2027. Se trata de una ley histórica porque es la primera del mundo que regula el campo emergente de la IA. Por eso, y al igual que ocurriera con el Reglamento General de Protección de Datos, este nuevo reglamento europeo puede marcar la pauta que sigan otros países. Y como es legalmente vinculante y establece multas por incumplimiento, sus consecuencias para las empresas transfronterizas son evidentes: basta recordar las multas que Bruselas impone una y otra vez a los gigantes tecnológicos estadounidenses por violar su normativa en multitud de materias, desde la privacidad hasta la fiscalidad o la competencia. Dadas las repercusiones globales de esta ley, Sampsa Samila, director de la Iniciativa sobre Inteligencia Artificial y el Futuro de la Dirección en el IESE, tenía muchas ganas de charlar con su arquitecto y autor principal, Gabriele Mazzini.

Mazzini no es el típico funcionario de carrera de Bruselas. Aunque empezó a trabajar para la UE en 2001, se tomó una excedencia en 2009 para cursar un máster en Estados Unidos, donde después acabó incorporándose al Millennium Villages Project, una iniciativa de desarrollo internacional que pretendía sacar de la pobreza a comunidades rurales de bajos ingresos valiéndose de las innovaciones tecnológicas. “Ahí fue donde nació mi interés por la tecnología y la normativa”, dice. Regresó a Europa en 2017 con el deseo de trabajar en las implicaciones normativas de las tecnologías emergentes. Cuando la IA comenzó a despegar, Mazzini era ya el más indicado para asesorar a la Comisión Europea sobre la confluencia de la IA y la legislación de la UE, así como para liderar la elaboración de una ley específica. Él atribuye a su estancia en Estados Unidos y a su experiencia laboral en diversas *startups* tecnológicas de ese país el hecho de tener una mentalidad emprendedora poco común en las instituciones europeas.

En esta entrevista, realizada poco antes de que entrara en vigor el reglamento de IA, en agosto pasado, Samila y Mazzini hablan de los pormenores de la ley, en especial del delicado equilibrio que debe articularse para controlar los riesgos que plantea la IA sin restringir en exceso la innovación.

Objetivos del Reglamento de Inteligencia

Artificial de la Unión Europea

Sampsa Samila: ¿Qué llevó a la Comisión a regular la IA?

Gabriele Mazzini: La Comisión quería asegurarse de que en toda la UE tuviéramos un conjunto de normas armonizadas para los productos y sistemas basados en la IA, de modo que su despliegue y uso cumpliera la legislación europea. Uno de los principios fundamentales de la UE es la libre circulación de bienes y servicios en su mercado interior, donde hemos de garantizar que se cumplen unos niveles mínimos de seguridad y se evitan impactos indeseados, como la discriminación ilegal, para que haya confianza entre empresas y ciudadanos. Por consiguiente, necesitábamos un marco legal común para evitar barreras entre los Estados miembros y proporcionar seguridad jurídica a las empresas que desarrollan sistemas de IA.

SS: ¿Cómo protege el reglamento de IA estos principios y derechos?

GM: Mediante tres categorías de riesgo. En primer lugar, si un sistema de IA plantea riesgos inaceptables, la ley prevé prohibirlo. Aquí se incluirían las aplicaciones que suponen una manipulación cognitiva del comportamiento, como los juguetes activados por voz que fomentan comportamientos peligrosos, o la puntuación social que categoriza a las personas no en función de prácticas consolidadas como la puntuación crediticia, sino de su “fiabilidad”, por ejemplo.

Segundo, puede haber sistemas de IA de alto riesgo relacionados con la contratación y gestión de empleados, la puntuación crediticia y la actividad policial, entre otras áreas, que amenacen con violar los derechos de las personas. Aunque permitidos, están sujetos al cumplimiento previo de determinados requisitos y a un procedimiento de evaluación de conformidad. La mayoría de las disposiciones del reglamento corresponden a esta categoría, que constituye la carga más importante para las empresas.

La tercera categoría afecta a los sistemas de IA con un riesgo ligado a la falta de transparencia o información, por ejemplo, si no se advierte a los usuarios que interactúan con la IA cuando hablan con un chatbot. Son cuestiones que atañen a la voluntad y dignidad de las personas, otro de los derechos fundamentales de la UE.

La estrategia de la UE para el desarrollo de la IA

SS: ¿Cómo encaja todo esto en el panorama más amplio del desarrollo de la IA en los Veintisiete?

GM: La estrategia europea de IA se basa en dos elementos que funcionan juntos: el ecosistema de confianza que he mencionado y otro de excelencia, que es básicamente la financiación y coordinación de la I+D entre los Estados miembros. Significa invertir en habilidades, nodos de innovación e instalaciones de pruebas para las empresas a través de programas como Horizonte Europa, una apuesta por la excelencia que complementa la confianza.

SS: ¿Cómo se ha procurado que la regulación no restrinja la innovación?

GM: Ese es el quid de cualquier regulación. La regulación puede apoyar la innovación sirviendo de orientación, pero toda norma es también una restricción. No creo que la regulación siempre apoye la innovación, pero sí que es el precio que tal vez haya que pagar con determinados tipos de innovación.

Debemos abordar este debate y cada jurisdicción tiene su propio enfoque. Estados Unidos es conocido por dejar que la innovación vaya más rápido y libre, para después valerse de medidas correctoras, impulsadas por el mercado, que los ciudadanos o las empresas pueden activar a través del sistema judicial, como por ejemplo la responsabilidad jurídica. En Europa solemos tener más aversión al riesgo, hasta tal punto que queremos prevenir las externalidades y consecuencias negativas desde el principio, cuando los posibles riesgos apenas se vislumbran. El coste potencial de este enfoque es restringir la innovación al fijar límites y salvaguardas mientras se desarrolla la innovación.

El reglamento trata de conseguir este equilibrio apoyándose en normas en lugar de entrar en detalles técnicos. Al exigir el cumplimiento normativo de las empresas en lo referente a gobernanza de datos, documentación, supervisión humana, transparencia y robustez, el reglamento mantiene un nivel bastante alto. Es una manera de permitir que la comunidad tecnológica siga desarrollando soluciones, pero cumpliendo esos requisitos, es decir, de apoyar tanta innovación en IA como sea posible dentro de un marco legal estable y basado en principios.

La regulación de la IA y las pequeñas empresas

SS: Preocupa que solo las empresas más grandes, en su mayoría no europeas, cuenten con los recursos necesarios para afrontar este tipo de regulación y los costes aparejados. ¿Cómo se facilita el crecimiento de las pymes europeas con menos recursos?

GM: No estoy seguro de que aquí hayamos logrado el equilibrio adecuado. Para ello, el trato a los actores pequeños debería haber sido distinto al de los grandes. Recuerdo que se debatió sobre si debía darse a las pymes un trato especial para reducirles las cargas financieras y de otro tipo. De hecho, se introdujeron disposiciones *ad hoc*, aunque limitadas. Pero, el enfoque, como eximir a ciertos actores del mercado de algunas normas hasta alcanzar un tamaño determinado, no me parece lo suficientemente audaz. Los Estados miembros y la Comisión deberían tomar medidas en materia de formación y canales de comunicación para facilitar la participación de los actores pequeños en el proceso de estandarización. Algo con lo que sí cuentan estos actores es el acceso prioritario a los *sandbox*, o entornos controlados de pruebas.

SS: ¿Cómo fomenta el *sandbox* la innovación?

GM: El *sandbox* ofrece a las empresas un marco general para desarrollar y testar sistemas de IA en un entorno controlado, supervisado por las autoridades. En este espacio seguro pueden innovar evitando determinados problemas, como las multas, y testar en condiciones reales (o sea, en un entorno libre), pero con ciertas salvaguardas.

Normativa para los modelos fundacionales

SS: ¿Cómo aborda el reglamento los modelos de propósito general o fundacionales, esos que están en desarrollo y cuyas aplicaciones y capacidades aún no entendemos del todo?

GM: Este tema generó un gran debate, sobre todo durante las negociaciones finales. De hecho, la propuesta inicial no incluía ninguna norma relativa a los modelos fundacionales. Pero, tras la aparición de ChatGPT, el Parlamento y el Consejo europeos acordaron abordar este nuevo fenómeno e introdujeron normas adicionales, aunque con un enfoque y perspectiva diferentes. Al final, existe un sistema de dos niveles, con normas para todos los modelos de propósito general y otras adicionales para los que presentan un riesgo sistémico.

Era crítico resolver cómo distinguir entre ambos tipos de modelos. Consideramos que el único criterio más o menos claro a seguir era la cantidad de poder computacional utilizado en su entrenamiento.

SS: ¿Por qué el cómputo y no el tamaño del modelo o el de los datos de entrenamiento?

GM: La Orden Ejecutiva sobre IA que la Administración Biden emitió en octubre de 2023 hace hincapié en la medición de las operaciones de punto flotante, o FLOPS, que está relacionada con el cómputo necesario para el entrenamiento de los modelos de IA. Fue decisivo para nosotros, pues entendimos que los FLOPS pueden considerarse como una especie de parámetro combinado que refleja otros factores, como la cantidad de datos de entrenamiento y los parámetros de modelo.

SS: Vemos modelos cada vez más potentes. ¿Existe algún mecanismo para actualizar ese umbral de cómputo?

GM: Sí. Era un elemento crucial que había que añadir para que la regulación fuera "a prueba de futuro". Este primer intento de la ley de cuantificar los FLOPS se puede modificar. La Comisión podrá cambiar ese umbral. Teniendo en cuenta que lo que hace dos años se consideraba un modelo de gran tamaño ya no lo es, los parámetros volverán a cambiar en el futuro.

El reglamento también prevé la posibilidad de que, al margen del umbral de cómputo, la Comisión determine que ciertos modelos plantean un riesgo sistémico basándose en un procedimiento aparte, el cual contempla otros factores incluidos en un anexo.

SS: ¿Por qué se han excluido los modelos de código abierto de la regulación de la IA de propósito general?

GM: En realidad, se han cubierto de forma menos estricta. Hay cuatro series de normas: la documentación técnica que provee de información a las autoridades, la transparencia con los proveedores descendentes y otras dos series de obligaciones en derechos de autor. Estas cuatro obligaciones son aplicables a los modelos de la IA de propósito general, solo que los de código abierto están exentos de dos: la documentación técnica y la transparencia. En cuanto a los modelos con riesgos sistémicos, existen obligaciones adicionales relativas a la evaluación y gestión de riesgos aplicables a todos ellos, tanto si son patentados como de código abierto.

Influencia mundial de los gigantes de la IA

SS: Hablemos sobre la aplicación e influencia global del reglamento. Voces como Yann LeCun que alertan del riesgo de que un puñado de gigantes tecnológicos dominen los modelos de IA, por muy seguros que sean, y controlen gran parte de nuestra vida y contenidos digitales.

GM: Coincido en su punto de vista. No queremos vivir en un mundo en el que nuestras preferencias estén influidas culturalmente por un puñado de personas y empresas. Queremos que haya una variedad de contenidos digitales y de preferencias basada en las distintas culturas. El objetivo de un menú digital justo y variado vendría a respaldar el argumento en favor del código abierto y no de los sistemas cerrados de unas pocas compañías.

El lema de la UE es "Unida en la diversidad". Necesitamos desarrollar modelos propios que atiendan nuestras lenguas y culturas. ¿Cómo vamos a esperar que una empresa no europea atienda mejor nuestra diversidad cultural? Los modelos fundacionales y, en particular, los de lenguaje constituyen un mercado emergente en el que la apertura es crucial. Además, aportan ventaja competitiva en primer lugar a nosotros, los Veintisiete, y más en general a quienes no tienen el inglés como lengua materna. En ese sentido, debemos procurar no cerrar el sistema, sino contar con actores locales que apoyen y sirvan a cada mercado lingüístico y respeten los matices culturales.

SS: Al margen de los asuntos relativos a los riesgos de seguridad, ¿propicia la regulación la toma en consideración de las especificidades culturales y políticas?

GM: Sí, aunque me pregunto si se han tomado lo suficientemente en cuenta los matices y el valor que Europa puede aportar en este ámbito, lo que no quiere decir que su reglamento de IA actúe de obstáculo. Es cierto que las normas más estrictas, las del nivel superior, son aplicables a los modelos con riesgos sistémicos, pero también tenemos una obligación para con el nivel inferior. Espero que en los próximos dos años crezca la necesidad de tener en cuenta los matices culturales y que eso garantice la competitividad de los actores europeos que desarrollan modelos en las lenguas de los Veintisiete.

UE, pionera en normas de IA

SS: Aparte de la Orden Ejecutiva de la Administración Biden, la Comisión Europea es el primer organismo gubernamental que regula en sentido estricto la IA. Ser el

primero, ¿es más bien un coste o un beneficio?

GM: Nos da la ventaja del pionero, en el sentido de que ponemos una pica en la regulación de la IA y, por tanto, obligamos a los demás a tenerla en cuenta. Como Europa es un mercado de gran tamaño, cualquier empresa que quiera operar en él debe cumplir sus normas. Eso compele a otras jurisdicciones –ya sea porque sus empresas operan en la UE o simplemente porque creen necesario regular ellos mismos la IA– a estudiar qué es lo que se hace aquí y decidir si adaptan la legislación europea en lugar de empezar de cero.

No discriminamos entre las empresas de aquí y las de fuera, porque lo importante cuando quieres vender un producto de alto riesgo en el mercado europeo es que rijan las mismas normas. No obstante, las empresas de los Veintisiete tendrán que afrontar el reglamento de IA y normas más estrictas en su mercado doméstico, mientras que las demás podrán desarrollar sus productos fuera de la UE sin tener que cumplirlo, por lo que crecerán antes de entrar en el mercado europeo. Las empresas van a afrontar estas normas en distintos momentos de su crecimiento, lo que nos lleva de nuevo a la cuestión de que las grandes compañías lo tendrán más fácil.

SS: ¿Cómo se garantiza la implementación y el cumplimiento del reglamento en todos los países miembros?

GM: Según el derecho comunitario, Bruselas elabora las leyes y los Estados miembros las aplican, salvo algunas excepciones. Con el reglamento de IA, la situación es un tanto ambivalente. Por un lado, están las autoridades nacionales de los Estados miembros. Puede darse el riesgo de que estas sean más o menos rígidas y que, por tanto, la aplicación del reglamento difiera, pero dicho riesgo queda mitigado por la existencia de un mecanismo de coordinación que, basado en el Reglamento de Vigilancia del Mercado, prevé que todas las autoridades de vigilancia del mercado se reúnan regularmente e intercambien buenas prácticas. Normalmente, alinean sus prácticas de aplicación legislativa. En caso de conflicto, la Comisión puede intervenir y decidir por todos.

SS: ¿Cómo mantiene esta regulación su vigor y relevancia a medida que las tecnologías de IA evolucionan?

GM: Es una de nuestras preocupaciones desde que empezamos, allá por 2019-2020. El reglamento regula una serie de tecnologías muy complejas y, como dices, la IA ha evolucionado con el tiempo. No hay consenso, ni siquiera entre los expertos, sobre qué es y qué no es IA. En medio de esta complejidad, ¿cómo se crea un marco legal que, por

definición, exige precisión? Debe quedar claro a qué tecnologías afecta la regulación.

Es un equilibrio difícil: por un lado, hay que proporcionar ya mismo seguridad jurídica a las empresas y, por el otro, permitir una adaptación flexible. Según el ordenamiento jurídico europeo, hemos de hacerlo ateniéndonos a un marco legal sólido y estable. Ello exige que los elementos esenciales de la ley los establezca el poder legislativo y no el ejecutivo, por lo general más ágil en su facultad normativa.

Es una dificultad inherente. La tecnología avanza muy rápido, mucho más que las medidas o revisiones legislativas. Solo la negociación del reglamento de IA ya llevó tres años. De todas formas, quizá el reglamento evolucione algo más rápido si se cambian algunos de sus mecanismos o principios estructurales. En ciertos aspectos, seguirá siendo un problema por resolver. Pero, desde luego, hacemos todo lo que podemos.

Esta entrevista se basa en dos conversaciones mantenidas el 21 de junio y 1 de julio de 2024, editadas por motivos de extensión y claridad.

Esta entrevista se publica en la revista IESE Business School Insight núm. 168 (sept.-dic. 2024).