Centre for Information Policy Leadership

HUNTON ANDREWS KURTH

Centre for Information Policy Leadership

Diez recomendaciones para la regulación global de la IA

Octubre de 2023

Centre for Information Policy Leadership
HUNTON ANDREWS KURTH

Diez recomendaciones para la regulación global de la IA

Contenido

INTRODUCCIÓN

La inteligencia artificial (IA)[i] está generando amplios y crecientes beneficios sociales, entre ellos el impulso de la investigación médica, el tratamiento del cambio climático, la transformación de las industrias y la modernización de los Gobiernos. Al mismo tiempo, el rápido despliegue y adopción de nuevas aplicaciones, como los chatbots generativos de IA y los generadores de imágenes, han intensificado preocupaciones duraderas y planteado nuevas preguntas relacionadas con privacidad y protección de datos, transparencia y capacidad de explicación, derechos humanos, propiedad intelectual, seguridad, prejuicios, repercusión en la mano de obra, generación y difusión de información errónea y desinformación y otros efectos sociales. En respuesta, las organizaciones están desarrollando controles operativos y marcos de gobernanza para garantizar el desarrollo y el despliegue responsables de la IA; los expertos de la industria están trabajando para desarrollar normas; los encargados de elaborar las políticas están redactando nuevas leyes; y los reguladores están poniendo a prueba los límites de las autoridades existentes y proponiendo otras nuevas[ii]. Sin embargo, no hay consenso entre los países sobre cuál es el mejor enfoque para regular la IA: ¿debería centrarse en una regulación estricta, en modelos de regulación conjunta, en certificaciones y garantías, en normas industriales o en alguna combinación?[iii]

Durante más de 20 años, el CIPL ha sido un líder de opinión en materia de responsabilidad organizacional y un enfoque basado en el riesgo para las políticas y las prácticas de datos, y fue uno de los primeros en contribuir a la determinación de los retos y la definición de soluciones para la gobernanza de la IA y las prácticas de la industria. Las principales contribuciones del CIPL en este ámbito incluyen *Artificial Intelligence and Data Protection in Tension* (octubre de 2018), *Hard Issues and Practical Solutions* (febrero de 2020) y *Artificial Intelligence and Data Protection: How the GDPR Regulates AI* (marzo de 2020)[iv]. El CIPL también ha preparado respuestas detalladas a consultas públicas sobre políticas de IA en Brasil, la Unión Europea, el Reino Unido y Estados Unidos[v].

Con base en esta experiencia y en nuestro amplio compromiso con los líderes del sector privado que desarrollan y despliegan tecnologías de IA, los encargados de elaborar las políticas y los reguladores, el CIPL ofrece en este documento diez recomendaciones para orientar la formulación de políticas y la regulación de la IA con el fin de permitir una IA responsable, seria y digna de confianza. Estas diez recomendaciones resumen la opinión del CIPL sobre un enfoque estratificado o a tres niveles de la regulación de la IA:

a) reglas basadas en principios y resultados;
b) responsabilidad organizacional demostrable, y
c) supervisión regulatoria sólida e inteligente.

Este enfoque proporciona reglas con garantía de futuro basadas en principios fundamentales que pueden guiar el desarrollo ético y el despliegue de la IA, incluso a medida que evolucionan la tecnología y los casos de uso. A continuación describimos este enfoque.

Recomendaciones para regular la IA

El CIPL recomienda un enfoque basado en el riesgo y por niveles para regular la IA que se base en las leyes y normas existentes y en las prácticas responsables de las organizaciones. Este enfoque debe estar respaldado por una supervisión regulatoria innovadora e instrumentos corregulatorios.

Cualquier planteamiento legislativo o regulatorio de la IA debe seguir estas recomendaciones generales:

A. Reglas basadas en principios y resultados
   1. Crear un marco flexible y adaptable que defina los resultados que deben alcanzarse, en vez de prescribir los detalles de cómo lograrlos.
   2. Adoptar un enfoque basado en el riesgo que considere los riesgos y los beneficios de forma holística.
   3. Apoyarse en fundamentos legales vinculantes y no vinculantes.
   4. Empoderar a las personas mediante mecanismos de transparencia, capacidad de explicación y rectificación.

B. Responsabilidad organizacional demostrable
   5. Hacer de la responsabilidad organizacional demostrable un elemento central de las regulaciones sobre IA.
   6. Avanzar en la adopción de prácticas responsables de gobernanza de la IA.
   7. Asignar la responsabilidad cuidadosamente, centrándose en la parte más estrechamente relacionada con la generación de perjuicio.

C. Supervisión regulatoria inteligente
   8. Crear mecanismos de coordinación y cooperación entre organismos regulatorios.
   9. Instituir una supervisión regulatoria basada en la cooperación y permitir la innovación regulatoria permanente.
   10. Luchar por la interoperabilidad global.

I. REGLAS BASADAS EN PRINCIPIOS Y RESULTADOS

1. Crear un marco flexible y adaptable que defina los resultados que deben alcanzarse, en vez de prescribir los detalles de cómo lograrlos.

Para ser eficaces, las regulaciones sobre IA deben poder seguir siendo pertinentes a medida que avanzan la tecnología y los casos de uso. Todas las reglas deben ser *neutrales con respecto a la tecnología*: un marco demasiado prescriptivo y específico para tecnologías específicas o modelos y prácticas comerciales actuales corre el riesgo de quedar rápidamente obsoleto e inhibir innovaciones beneficiosas. De hecho, un enfoque basado en listas de tecnologías específicas requerirá frecuentes modificaciones para mantenerse al día con los cambios tecnológicos. Si las reglas incluyen listas de tecnologías y aplicaciones presuntamente de alto riesgo, deben permitir que esas presunciones sean refutables y evolucionen con el tiempo.

Las reglas también deben *basarse en principios y resultados*. Deben permitir a las organizaciones

garantizar los resultados requeridos (p. ej., imparcialidad, ausencia de prejuicios, transparencia, precisión, seguridad, supervisión humana, etc.) a través de políticas, procedimientos y controles internos verificables y basados en el riesgo, que sean apropiados en sus contextos específicos, sin prescribir cómo lograr estos resultados. Este enfoque ofrece a los desarrolladores la flexibilidad necesaria para innovar, incluida la capacidad de innovar en controles reales, herramientas técnicas y salvaguardias, manteniendo al mismo tiempo la coherencia con los principios básicos y los resultados[vi].

Del mismo modo, un marco regulatorio no debe ser excesivamente prescriptivo en cuanto a las metodologías de evaluación del efecto y el riesgo de la IA, sino describir los criterios que deben tenerse en cuenta al evaluar los riesgos y beneficios de una aplicación de IA y dejar que los reguladores competentes proporcionen más orientaciones adaptadas, realistas y prácticas en colaboración con quienes desarrollan y despliegan las tecnologías de IA.

Al mismo tiempo, las reglas deben ofrecer la mayor seguridad posible en cuanto a su ámbito de aplicación. Por ejemplo, un marco regulatorio de la IA debe definirla para que las partes interesadas puedan entender claramente qué sistemas están cubiertos por las reglas. A falta de dicha claridad y de un enfoque basado en los resultados, la ambigüedad regulatoria y el exceso de prescripción corren el riesgo de inhibir la inversión y la innovación, especialmente para las pequeñas y medianas empresas (PYME) y las empresas emergentes, que son potentes motores de la innovación y la inversión en IA.

2. Adoptar un enfoque basado en el riesgo que considere los riesgos y los beneficios de forma holística

Cualquier enfoque regulatorio de la IA debe tratar de proteger los derechos humanos fundamentales y minimizar los riesgos para las personas y la sociedad, permitiendo al mismo tiempo el desarrollo y el uso de la IA en beneficio de ambos. De hecho, los riesgos para las personas y la sociedad también pueden materializarse por *no* utilizar tecnologías de IA eficaces, como las que tienen capacidad para predecir y prevenir enfermedades o para reducir los perjuicios en línea, las amenazas a la ciberseguridad y el fraude. Un enfoque holístico basado en el riesgo promueve esta meta facilitando medidas de protección prácticas que sean proporcionales a los riesgos y beneficios de un sistema de IA particular. Se centra en las posibles repercusiones de la tecnología de IA en el contexto de casos de uso específicos.

Un marco regulatorio de la IA basado en el riesgo proporcionaría criterios no exhaustivos para ayudar a las organizaciones a determinar la probabilidad y gravedad de cualquier perjuicio resultante y las medidas necesarias para mitigarlo. Evaluar y comprender el efecto potencial de sus aplicaciones de IA permite a las organizaciones adaptar sus mitigaciones a los riesgos reales y evitar la implementación de medidas innecesarias. Por ejemplo, el algoritmo de k vecinos más cercanos (k-nearest neighbors, KNN) es un algoritmo de aprendizaje automático que se utiliza en una variedad de aplicaciones[vii]: en el comercio minorista para recomendar productos, en la atención médica para predecir el riesgo de infarto y cáncer de próstata, en las finanzas para detectar actividades fraudulentas, en la agricultura para predecir el rendimiento de las cosechas y en el transporte para predecir y optimizar el tráfico. Estos diferentes usos del mismo algoritmo KNN tienen diferentes niveles de riesgo: la probabilidad y gravedad del perjuicio en la recomendación de canciones o ropa difieren de las que se usan en la medicina de emergencia.

Un marco basado en el riesgo también debe evaluar los beneficios potenciales de un sistema de IA para las personas, las organizaciones y la sociedad. A continuación, pueden sopesarse con los riesgos identificados de desplegar (o no) la IA. Por ejemplo, los riesgos de los vehículos autónomos (autonomous vehicles, AV) dependen de los distintos entornos en los que se despliegan. Podría decirse que el riesgo de que los vehículos autónomos causen perjuicios a las personas es menor en la minería y la agricultura que en las zonas urbanas o residenciales. Al mismo tiempo, los vehículos autónomos en los entornos

anteriores ofrecen diferentes beneficios, como facilitar la oferta de mano de obra, apoyar la agricultura sostenible y mejorar la productividad[viii]. El mismo ejemplo es útil para resaltar la importancia de sopesar cuidadosamente las métricas para medir el riesgo: se podría evaluar el riesgo de los AV frente al *statu quo* (un mundo en el que la mayoría de los autos son conducidos por personas) o una norma óptima designada para los AV.

En resumen, los resultados de las evaluaciones holísticas de riesgos para el uso de una tecnología de IA específica pueden variar significativamente según los casos de uso. Desde la perspectiva de la elaboración de políticas, esto significa que puede ser difícil identificar definitivamente los usos de alto o bajo riesgo de antemano, ya que el contexto de despliegue es clave. Un enfoque basado en el riesgo es preferible a un enfoque categórico que defina los sistemas de IA que se consideran automáticamente de alto riesgo. Por ejemplo, considerar de alto riesgo todos los sistemas de IA que hacen inferencias basadas en datos biométricos podría abarcar usos auxiliares de riesgo relativamente bajo, como cuando se utiliza la IA para aplicar filtros o mejorar la calidad de video en las videollamadas.

Un enfoque más adecuado sería:

A) describir factores, criterios y perjuicios potenciales que deben tener en cuenta las evaluaciones de riesgos;
B) proporcionar, a lo sumo, una lista ilustrativa de usos potencialmente de mayor o menor riesgo que puedan rebatirse en cada caso particular;
C) proporcionar orientación continua sobre cómo evaluar los riesgos y beneficios basándose en lo aprendido a lo largo del tiempo.

3. Apoyarse en fundamentos legales vinculantes y no vinculantes

Un régimen de IA flexible y adaptable debe basarse en los marcos legales existentes, incluidos las regulaciones y la legislación ("leyes vinculantes") y las "leyes no vinculantes" (p. ej., los Principios de la IA de la OECD). Muchos de los sectores en los que se aplica la IA ya están muy regulados (p. ej., la atención médica o las finanzas) y las leyes y regulaciones vigentes ya establecen requisitos, estructuras de cumplimiento y soluciones que rigen al uso de la IA. Sin embargo, es posible que las leyes y regulaciones vigentes también deban interpretarse de una nueva manera y adaptarse a las realidades de la IA. Cuando existan brechas regulatorias sobre los riesgos relacionados con la IA, deben cerrarse con una intervención regulatoria y corregulatoria específica, dando prioridad a los sectores en los que no se apliquen las regulaciones existentes.

Basarse, en la medida de lo posible, en los marcos de la ley vinculante existente reduce el riesgo de crear reglas superpuestas o contradictorias que podrían generar inseguridad legal y protecciones incoherentes. Las reglas existentes en materia de antidiscriminación, protección de los consumidores, propiedad intelectual y, lo que es más importante, protección de datos y privacidad son pertinentes para abordar muchos de los riesgos más importantes que se asocian con la IA. Por ejemplo, en marzo de 2020, el CIPL elaboró un análisis exhaustivo en el que describía cómo la Regulación General de Protección de Datos de la UE ya regula la IA en relación con el uso de datos personales[ix]. Cuando existen brechas en los marcos legislativos —como en Estados Unidos, que actualmente carece de una ley federal exhaustiva sobre privacidad—, cerrarlas es una base importante para una regulación sólida de la IA[x]. Cuando los marcos existentes son pertinentes, los organismos regulatorios pueden fomentar el cumplimiento publicando orientaciones sobre cómo se aplican esas reglas a la IA. Mediante la consulta con una serie de partes interesadas, los reguladores pueden identificar las circunstancias en las que dicha orientación será más útil.

Además, es importante reconocer que las reglas existentes pueden requerir cierta adaptación y una

interpretación regulatoria evolucionada para alinearlas con la evolución de la tecnología de la IA. Por ejemplo, algunos principios que se recogen en muchas leyes de protección de datos, como la base legal del procesamiento, la especificación de la finalidad y la limitación del uso, pueden entrar en tensión con las necesidades de los sistemas de IA y su funcionamiento.

En cuanto al concepto de base legal, puede que no haya suficientes bases legales en las actuales leyes de protección de datos para permitir a los desarrolladores de IA utilizar categorías sensibles de datos personales, como la salud, el sexo y la etnia, para garantizar que el modelo de IA está probado y funciona de una manera que no genera resultados prejuiciados o discriminatorios. Además, si los datos personales se tratan sobre la base de un fundamento legal específico para finalidades específicas, y se utilizan solo para esas finalidades o para otras "compatibles", a menudo con interpretaciones restrictivas de lo que constituye "compatible", puede contradecir la naturaleza de cómo funcionan y aprenden los algoritmos de la IA. Dado el potencial de la IA de descubrir usos nuevos e imprevistos de los datos, estos principios pueden frustrar innecesariamente aplicaciones beneficiosas de la IA, a menos que se les dé una interpretación más amplia en el contexto de la IA. Un ejemplo de esta interpretación más amplia sería aplicar una definición más amplia de "compatible" que incluya cualquier finalidad que no anule o entre en conflicto con la finalidad inicial y no aumente el riesgo de perjuicio para las personas. Otra solución sería considerar la preparación algorítmica como una finalidad en sí misma, separad de la finalidad de desplegar el algoritmo para un caso de uso particular. Esto permitiría una recopilación y un uso más amplios de los datos en la fase de preparación para garantizar la preparación y el funcionamiento adecuados del algoritmo. Por último, surgen tensiones similares con respecto a los principios de minimización de datos y limitación de retención, que pueden limitar las oportunidades de los algoritmos de "aprender" mediante el reconocimiento de correlaciones. En resumen, si ciertos principios tradicionales de protección de datos se interpretan con demasiada rigidez, pueden bloquear el desarrollo y despliegue de aplicaciones beneficiosas de IA, o tener consecuencias no deseadas, como la introducción de prejuicios no deseados, al limitar el acceso a datos de preparación diversos[xi]. Los reguladores deben ser capaces de hacer evolucionar la interpretación de los principios de protección de datos existentes a través de orientaciones regulatorias elaboradas en consulta con los desarrolladores y los encargados del despliegue de la IA.

Por último, las reglas existentes deben complementarse con marcos legales no vinculantes, normas de la industria y herramientas corregulatorias desarrolladas en colaboración con las partes interesadas, como códigos de conducta, certificaciones y modelos de garantía. Las normas internacionales pueden ayudar a establecer unos requisitos básicos para el desarrollo y despliegue de la IA que reflejen los entendimientos y valores compartidos a los que se ha llegado a través de procesos de desarrollo en los que participan varias partes interesadas. Los Ministros de Tecnología y Asuntos Digitales del G7 reafirmaron la función clave de las normas en su Cumbre de Hiroshima de abril de 2023[xii] y acordaron en septiembre elaborar un Código de Conducta para las organizaciones que desarrollan sistemas avanzados de IA[xiii], mientras que el Grupo de Trabajo de Certificación, formado por varias partes interesadas, está liderando un trabajo prometedor sobre la Certificación de IA.[xiv] Aprovechar marcos legales no vinculantes como los Principios de la IA de la OECD puede fomentar la armonización internacional de las regulaciones sobre IA: por ejemplo, la versión del Parlamento de la Ley de IA de la UE deriva su definición de "Inteligencia Artificial" de esos principios.

4. Empoderar a las personas mediante mecanismos de transparencia, capacidad de explicación y rectificación

El CIPL ha abogado por el empoderamiento individual como principio básico de una regulación sólida de la privacidad, y lo mismo puede decirse de la IA. Para que la IA sea digna de confianza y beneficiosa para todos, las regulaciones, los marcos corregulatorios y las prácticas de la industria

deben empoderar a las personas mediante lo siguiente:

- **Transparencia.** Los desarrolladores y los encargados del despliegue de la IA deben proporcionar una transparencia significativa y adecuada al contexto sobre las entradas y operaciones de los sistemas de IA, preservando al mismo tiempo la privacidad y la protección de datos, la seguridad y los secretos comerciales. Esta transparencia contextualizada debería extenderse a los usuarios comerciales de los sistemas de IA, los auditores, los reguladores y el público en general.

    - Los **sistemas de IA de alto riesgo** deben documentar cómo está previsto que se utilice el sistema, los usos inadecuados y los riesgos conocidos, así como recomendaciones para los encargados del despliegue sobre cómo gestionar esos riesgos.
    - La **IA generativa** requiere medidas para garantizar que los usuarios comprendan las prácticas y limitaciones de los datos de los modelos. Lo ideal sería que los desarrolladores y los encargados del despliegue ofrecieran transparencia a través de varios mecanismos, como políticas, condiciones de servicio, notificaciones dentro del producto y centros de recursos centralizados.

- **Capacidad de explicación.** La capacidad de explicación es un aspecto de la transparencia y un medio de impulsar la responsabilidad y la confianza. Exige que los desarrolladores y los encargados del despliegue expliquen de manera significativa cómo los sistemas de IA afectan las decisiones y los resultados que influyen en las personas, teniendo en cuenta al mismo tiempo las ventajas y desventajas, por ejemplo, entre la capacidad de explicación y la seguridad y entre la capacidad de explicación y la precisión. Cuanto más complejo y preciso sea el algoritmo, más difícil será explicar cómo funciona realmente. También puede haber limitaciones técnicas a la capacidad de explicación en algunas circunstancias. Por ejemplo, no siempre es posible explicar cómo los grandes modelos lingüísticos (large language models, LLM) generan resultados específicos basados en entradas individuales o parámetros del modelo. Las organizaciones tendrán que documentar las compensaciones pertinentes para demostrar cómo y por qué han priorizado la precisión frente a la capacidad de explicación. Un ejemplo de ello pueden ser los algoritmos de IA que se utilizan en la atención médica y la medicina, donde la IA puede permitir ciertos beneficios para la salud que no se consiguen con herramientas ajenas a la IA, pero que pueden no ser explicables. En esas circunstancias, la precisión puede primar sobre la capacidad de explicación. En resumen, dependiendo del contexto, los riesgos y los beneficios potenciales de un caso de uso específico, exigir la plena capacidad de explicación como condición de uso puede no ser apropiado en todos los casos.

- **Comentarios de los usuarios y rectificación.** Cuando una persona no entienda una decisión que tome la IA, o crea que ha sido perjudicada por ella, debe haber opciones claras para que el usuario opine, pregunte, reclame, aumente la transparencia, tenga derecho a impugnar la decisión, se exija una revisión humana y, en última instancia, una rectificación, así como la actuación de las autoridades encargadas de hacer cumplir la ley, cuando sea apropiado y necesario. Los desarrolladores y los usuarios comerciales deben considerar cómo permitir una mayor transparencia, la revisión humana en caso de un uso impugnado de la IA, así como oportunidades para la captación de reclamos y la rectificación como parte del diseño de soluciones de extremo a extremo que aprovechan la IA.

II. RESPONSABILIDAD ORGANIZACIONAL DEMOSTRABLE

5. Hacer de la responsabilidad organizacional demostrable un elemento central de las regulaciones sobre IA

Para garantizar la responsabilidad dentro del ecosistema más amplio, las regulaciones deben facilitar el uso demostrable por parte de las organizaciones de marcos de responsabilidad y programas de gobernanza que proporcionen las herramientas y los procesos para que las organizaciones apliquen todos los requisitos legales pertinentes y otras normas. Al igual que en otros ámbitos del cumplimiento corporativo y la ética comercial tradicionales —y más recientemente en las esferas de los datos, la seguridad y lo digital—, la responsabilidad debe integrarse y aplicarse en todas las fases del ciclo de vida de la IA y la "pila tecnológica" de la IA, incluida la infraestructura del centro de datos, los modelos y las aplicaciones de la IA.[xv]

Hay diversos marcos de responsabilidad que proporcionan modelos útiles para diseñar programas de responsabilidad y gobernanza de la IA en las organizaciones, como el Marco de Gestión de Riesgos de la IA del NIST de EE. UU., el Marco Modelo de Gobernanza de la IA de Singapur y el propio Marco de Responsabilidad del CIPL que se describe en los Anexos 1-3 de este informe.[xvi]

Las organizaciones también tienen que ser capaces de *demostrar* su responsabilidad internamente (ante sus directivos y consejos corporativos) y externamente (ante accionistas, inversores, reguladores y el público en general). Certificaciones, auditorías, códigos de conducta y evaluaciones son herramientas útiles para demostrar responsabilidad. De hecho, estos mecanismos de responsabilidad son esenciales en las políticas y la regulación digitales, incluso para los desarrolladores y los encargados del despliegue de inteligencia artificial, por las siguientes razones:

- Demuestran a todos los agentes de la organización el compromiso y la capacidad de garantizar que los productos y servicios cumplen criterios específicos.
- Permiten a las organizaciones traducir los requisitos legales basados en principios y resultados en controles demostrables y basados en riesgos, garantizando una regulación más eficaz y un mejor cumplimiento en la práctica.
- Desempeñan una función importante a la hora de proporcionar seguridad legal y reforzar la confianza, incluso en contextos entre empresas.

Cualquier regulación de la IA debe incluir explícitamente la responsabilidad demostrable como elemento central, así como permitir el desarrollo y el uso de marcos corregualtorios, como sistemas de certificación y códigos de conducta, que faciliten y demuestren dicha responsabilidad.

6. Avanzar en la adopción de prácticas responsables de gobernanza de la IA

Aunque debería exigirse un conjunto básico de prácticas de responsabilidad a las organizaciones que desarrollan y despliegan IA, los encargados de elaborar las políticas y los reguladores también deberían fomentar e incentivar de forma proactiva la adopción de prácticas, marcos, herramientas y tecnologías de responsabilidad más amplios. Deben trabajar con las partes interesadas para desarrollar conjuntamente herramientas y marcos para crear y demostrar la responsabilidad de la IA. La meta debe ser crear un entorno en el que las organizaciones vean la adopción de marcos de responsabilidad bien desarrollados como elementos diferenciadores para crear valor y reforzar la confianza en sus prácticas de datos, más allá del cumplimiento de las obligaciones legales y regulatorias básicas.

Los encargados de elaborar las políticas y los reguladores también deben comprender los factores que impulsan y los retos que plantean las prácticas tecnológicas responsables y las soluciones

tecnológicas, como las tecnologías de mejora de la privacidad (Privacy Enhancing Technologies, PET), y tomar medidas para incentivar su desarrollo y adopción[xvii].

Debe considerarse una amplia gama de incentivos potenciales para la responsabilidad[xviii], entre los que se incluyen:

- Reconocer formalmente la responsabilidad demostrada o certificada como factor atenuante en las acciones de aplicación y en la evaluación de las sanciones o los niveles de las multas.
- Utilizar la responsabilidad demostrada como una forma de "licencia para operar", dando a las organizaciones responsables mayor libertad para desarrollar y desplegar modelos de IA de forma responsable.
- Permitir un uso más amplio de los datos en proyectos de IA para investigaciones socialmente beneficiosas que hayan sido validadas por evaluaciones de riesgos, mitigaciones, supervisión y controles pertinentes en programas de responsabilidad.
- Permitir a las partes que adquieran sistemas de IA cumplir los requisitos de debida diligencia mediante la adquisición de sistemas que hayan sido certificados conforme a normas reconocidas de IA responsable.
- Utilizar la responsabilidad demostrada en materia de IA como criterio de elegibilidad para los proyectos de contratación pública, a fin de incentivar a los contratistas para que obtengan la certificación de IA responsable.

7. Asignar la responsabilidad cuidadosamente, centrándose en la parte más estrechamente relacionada con la generación de perjuicio

La adopción de mecanismos organizacionales de responsabilidad por parte de todos los actores del ecosistema de la IA redundará en un mejor cumplimiento y mejores resultados sobre el terreno, y probablemente hará menos necesario plantear preguntas relacionadas con la responsabilidad. Sin embargo, en los casos en los que la responsabilidad plantea preocupaciones, se está debatiendo activamente sobre la distribución adecuada entre las partes del ecosistema de la IA.

En principio, la responsabilidad debe asignarse principalmente a la parte más estrechamente relacionada con la generación del perjuicio en cuestión, pero asignar la responsabilidad puede resultar complejo en la práctica. El análisis vendrá determinado por las normas legales y los precedentes existentes, así como por el grado en que las partes divulgan la información pertinente a través de los requisitos de transparencia e información.

Según las circunstancias, la responsabilidad puede asignarse al desarrollador, al encargado del despliegue, a los usuarios finales o a una combinación de ellos. Los desarrolladores podrían ser el foco apropiado de responsabilidad por sistemas que no han sido suficientemente probados para detectar posibles perjuicios o que se han proporcionado a los usuarios indicaciones engañosas sobre sus capacidades. Por otra parte, los usuarios comparten la responsabilidad de cómo utilizan los sistemas de IA, ya que determinan si emplean un sistema para un uso de mayor riesgo o de formas expresamente contraindicadas por las orientaciones proporcionadas por los desarrolladores.

Al igual que en otras áreas del comercio, los contratos —incluidas las nuevas prácticas contractuales específicas de la IA— desempeñarán una función importante en la distribución de las responsabilidades de las partes en el ciclo de vida del desarrollo e despliegue de la IA. Por ejemplo, si un desarrollador prohíbe contractualmente un caso de uso de alto riesgo de su producto, el riesgo de uso indebido debería trasladarse al usuario que haya incumplido intencionalmente las

condiciones de ese contrato. En los casos en que terceras partes proporcionen modelos de IA o soluciones basadas en IA, la responsabilidad entre los desarrolladores de modelos y los encargados del despliegue debe especificarse en los contratos.

III. SUPERVISIÓN REGULATORIA INTELIGENTE

8. Crear mecanismos de coordinación y cooperación entre organismos regulatorios

La IA se utiliza en sectores que se rigen por diferentes regulaciones y reguladores. Por ejemplo, las autoridades de protección de datos (data protection authorities, DPA) tendrán competencia general sobre el tratamiento de datos personales mediante IA. Otros reguladores tienen competencias más sectoriales sobre las aplicaciones de la IA, como en atención médica, vivienda, servicios financieros, telecomunicaciones y productos farmacéuticos y en disciplinas transversales como la propiedad intelectual. En la mayoría de los casos, no debería ser necesario un nuevo regulador general de la IA, ya que ello probablemente ocasionaría excesos regulatorios, solapamientos, incoherencias y falta de seguridad legal. Más bien, es más apropiado:

a) mejorar las competencias y capacidades de los reguladores existentes para que estén preparados para la vigilancia y supervisión de la IA, y
b) permitir la coordinación y colaboración a alto nivel de las políticas de IA entre las autoridades existentes.

Si bien cada regulador debe mantener la competencia sobre sus propias atribuciones (p. ej., a efectos de seguridad legal, las DPA deben mantener la competencia general sobre las aplicaciones de la IA que involucren el tratamiento de datos personales o afecten a la privacidad de las personas), debe crearse un organismo central permanente de coordinación gubernamental para establecer políticas y metas de alto nivel en materia de IA aplicables en todos los sectores e industrias y facilitar la alineación, la coordinación regulatoria y la acción conjunta entre los diferentes organismos regulatorios, cuando sea necesario y adecuado. El organismo de coordinación puede ofrecer a los reguladores un espacio en el que debatir las compensaciones entre los distintos objetivos de las políticas, como la eficiencia, la productividad, la equidad, la privacidad, la seguridad y la resiliencia. También puede aclarar a quién deben dirigirse las partes en busca de orientación en circunstancias específicas de desarrollo e despliegue de la IA.

Este enfoque sería beneficioso tanto para las organizaciones como para los reguladores, ya que fomentaría la coherencia de los enfoques regulatorios, así como políticas y orientaciones holísticas e interdisciplinarias más fáciles de implementar y de supervisar por parte de los reguladores especializados y de la industria a lo largo del tiempo. Este enfoque también puede ser útil para armonizar las nuevas leyes y reglamentos con los ya existentes.

Un ejemplo de coordinación interreculatoria es el Foro de Cooperación sobre Regulación Digital del Reino Unido (Digital Regulation Cooperation Forum, DRCF). Incluye un director general (Chief Executive Officer, CEO) y personal permanentes, actividades conjuntas, orientación conjunta y otras medidas regulatorias, así como proyectos formales de colaboración y comisiones de servicio de personal. La IA ha sido uno de los focos de atención del DRCF, como demuestra su línea de trabajo plurianual sobre transparencia algorítmica[xix]. Otros países, como Australia, Francia, Irlanda y los Países Bajos, también han establecido mecanismos de cooperación para los reguladores[xx].

9. Instituir una supervisión regulatoria basada en la cooperación y permitir la innovación regulatoria permanente

A medida que la tecnología sigue evolucionando, los reguladores, las técnicas y las herramientas regulatorias deben evolucionar también.

a) Los reguladores deben mejorar sus capacidades y su forma de actuar en un mundo en el que hay múltiples intereses en juego. Por ejemplo, la tarea de las autoridades de protección de datos no debe limitarse a proteger los derechos fundamentales de las personas, sino que también debe permitir un uso responsable de los datos y el desarrollo de la tecnología de la IA en beneficio de la sociedad y la economía de forma que se protejan los derechos fundamentales. Esto requiere un cambio en la mentalidad, las prioridades y las medidas regulatorias. Este cambio es esencial para que los reguladores actuales sigan siendo pertinentes y eficaces en un nuevo mundo digital.

b) Los reguladores deben adoptar un enfoque basado en el riesgo para ser estratégicos y eficaces. Esto requiere comprender los riesgos y beneficios de los sistemas de IA y centrarse en las áreas que presentan los mayores riesgos para las personas y la sociedad, preservando al mismo tiempo los beneficios de la tecnología de IA y su avance. También exige que los reguladores prioricen todo su trabajo —estrategia regulatoria, orientación, supervisión y cumplimiento— y se centren en las áreas que crean los mayores riesgos para las personas y la sociedad.

c) Los mecanismos tradicionales de supervisión, basados exclusiva o principalmente en la aplicación *ex post*, pueden no ser suficientes en una sociedad digital y basada en la inteligencia artificial. Confiar en solucionar los fallos del mercado únicamente mediante el cumplimiento de la ley no dará los resultados deseados. Dado el ritmo de avance de la tecnología de IA y la necesidad de comprender sus riesgos y beneficios, existe una necesidad acuciante de un enfoque más cooperativo basado en un compromiso constructivo continuo entre los reguladores y las entidades regulatorias, el intercambio de experiencias e información sobre los avances tecnológicos y el trabajo conjunto para desarrollar objetivos de cumplimiento realistas e interpretaciones de las reglas correspondientes. Esto requiere que tanto los reguladores como las entidades regulatorias sean transparentes y estén dispuestos a compartir información constructiva en tiempo real a medida que cambian las tecnologías y las prácticas comerciales.[xxi] Es probable que invertir en medidas *ex ante*, como incentivar la responsabilidad proactiva y demostrable, logre mejores resultados que una costosa aplicación *ex post*. Por supuesto, el cumplimiento debe seguir siendo una opción regualtoria y una palanca importante en caso de infracciones reiteradas, graves y negligentes que causen un perjuicio real a las personas y a la sociedad.

d) Las herramientas regulatorias innovadoras, como los entornos aislados y la elaboración de prototipos de políticas, pueden ser eficaces para la supervisión regulatoria de nuevas tecnologías como la IA. Proporcionan a los reguladores un conocimiento más profundo y una experiencia de primera mano de las aplicaciones y desarrollos de la IA, dirigidos al mercado general. También prevén un puerto seguro para que la industria pruebe los riesgos y beneficios de la innovación responsable con un vínculo directo con el regulador competente. Los Gobiernos deben proporcionar financiamiento y recursos adecuados para que los reguladores desarrollen y participen en entornos aislados regulatorios y puedan extender estas actividades a un grupo más amplio de participantes, incluso a escala sectorial.

Entornos aislados regulatorios: los entornos aislados regulatorios son mecanismos importantes para la exploración y experimentación regulatoria, ya que proporcionan un banco de pruebas para aplicar las leyes a productos y servicios innovadores en entornos reales bajo la supervisión de un

regulador.[xxii] Pueden utilizarse para ayudar a abordar y resolver algunos de los aspectos más difíciles del despliegue de la IA en el contexto de los requisitos legales vigentes, en particular los que parecen incoherentes o en tensión con las nuevas tecnologías. Algunos ejemplos son:

- Desde 2020, la Oficina del Comisionado de Información del Reino Unido cuenta con un programa de entorno aislado, centrado especialmente en las tecnologías emergentes y la biometría[xxiii].
- La Autoridad de Desarrollo de Medios de Información y Comunicación (Infocomm Media Development Authority, IMDA) de Singapur permite a las empresas obtener orientación regulatoria para tecnologías innovadoras que hacen un uso intensivo de datos. La IMDA también gestiona un entorno aislado específico para fomentar el desarrollo y la adopción de tecnologías de mejora de la privacidad (PET)[xxiv].
- La Autoridad Noruega de Protección de Datos (Datatilsynet) puso en marcha un entorno aislado regulatorio especial para aplicaciones de IA[xxv].
- El Gobierno colombiano desarrolló un entorno aislado regulatorio para promover la privacidad por diseño y por defecto en los proyectos de IA[xxvi].
- La Comisión Nacional de Tecnologías de la Información y Libertades (CNIL) de Francia opera un entorno aislado que ha completado proyectos en los ámbitos de la salud digital y la tecnología educativa. En 2023, anunció una nueva iniciativa centrada en la IA[xxvii].
- El proyecto de Ley de IA de la UE permitiría, y en última instancia podría obligar, a los estados miembros a crear entornos aislados regulatorios de IA. España fue el primer estado miembro en poner a prueba un entorno aislado de IA[xxviii].

Los entornos aislados regulatorios deben diseñarse de forma que fomenten la innovación, el intercambio de información y otros modos de cooperación. Cualquier marco regulatorio de la IA debe proporcionar una base estatutaria explícita para que los reguladores establezcan entornos aislados, incluidos los entornos aislados interregulatorios con los reguladores apropiados y pertinentes, como los de protección de datos, competencia, medios de comunicación, consumidores, salud y farmacia, telecomunicaciones y finanzas. Las regulaciones deben tener en cuenta cómo las autoridades legales o las prioridades de cumplimiento pueden afectar la participación de las compañías. Al mismo tiempo, para garantizar la confianza del público en los resultados, los entornos aislados deben incluir garantías de que los individuos seguirán estando protegidos de los perjuicios incluso mientras se experimenta con las políticas.

Prototipos de políticas: se trata de proyectos piloto que movilizan a agentes públicos y privados para explorar, evaluar y desarrollar conjuntamente diferentes modelos legislativos de gobernanza antes de su promulgación efectiva. El proceso suele involucrar la selección de un grupo de participantes, como compañías tecnológicas en fase inicial, para desarrollar y aplicar prototipos de políticas en colaboración con expertos gubernamentales, industriales y académicos. El programa OpenLoop de Meta ha sido uno de los principales practicantes de la creación de prototipos de políticas, incluida la propuesta de Ley de IA de la UE. [xxix] La IMDA de Singapur cuenta con un programa de creación de prototipos de políticas dentro de su entorno aislado regulatorio de datos que se ha centrado en la notificación, el consentimiento y la divulgación; la transparencia y la capacidad de explicación de la IA; y la transparencia y el consentimiento en el metaverso, incluidos los contextos para la aplicación del interés legítimo como base para el tratamiento[xxx].

10. Luchar por la interoperabilidad global

Dada la naturaleza global de la tecnología de IA —desde los datos que utiliza para la preparación hasta la investigación y el desarrollo, la infraestructura informática y las aplicaciones que cruzan fronteras—, está claro que ningún Gobierno puede abordar satisfactoriamente la política y la regulación de la IA de forma aislada. La cooperación a nivel internacional es esencial para garantizar que las personas y las sociedades de todo el mundo puedan confiar en los beneficios de una IA digna de confianza y responsable y que los nuevos riesgos se evalúen y mitiguen de forma continua. Este trabajo se beneficiaría de un foro internacional específico que permitiera a los Gobiernos y otras partes interesadas cooperar en las políticas de la IA.

Además, la cooperación internacional debe fomentar la interoperabilidad de las políticas y regulaciones sobre IA. Como ha señalado el CIPL en el contexto de la protección de datos, la interoperabilidad global permite la prestación responsable de servicios transfronterizos, amplía el acceso, reduce los costos de cumplimiento, aumenta la seguridad legal y garantiza una protección coherente de los derechos e intereses de las personas.[xxxi] Las distintas jurisdicciones tendrán sus propias prioridades, tradiciones legales y cuerpo regulatorio existente, pero pueden unirse en torno a principios y enfoques básicos a la hora de considerar las políticas y la regulación de la IA, similares a los que el CIPL presenta en este documento. También pueden tomar medidas para codificar la interoperabilidad a través de mecanismos de reconocimiento y certificación, incluida la participación en el sistema de Reglas Globales de Privacidad Transfronteriza (Global Cross-Border Privacy Rules, CBPR) en el contexto de la protección de datos y los flujos transfronterizos de datos confiables[xxxii]. Ha habido esfuerzos alentadores hacia la interoperabilidad de la IA a través de la iniciativa del G7 antes mencionada, los Principios de la IA de la OCDE,[xxxiii] acuerdos comerciales y económicos, como el Acuerdo de Asociación de Economía Digital (Digital Economic Partnership Agreement, DEPA)[xxxiv] y la Asociación Global sobre IA.[xxxv]

ANEXO I - MARCO DE RESPONSABILIDAD DEL CIPL

ANEXO II - ADAPTACIÓN DE LAS MEJORES PRÁCTICAS DE GOBERNANZA DE LA IA AL MARCO DE RESPONSABILIDAD DEL CIPL

En la siguiente tabla se presentan ejemplos de actividades de responsabilidad en materia de IA llevadas a cabo por organizaciones seleccionadas de diferentes sectores, zonas geográficas y tamaños, basadas en el Marco de responsabilidad del CIPL y clasificadas en función de cada elemento de responsabilidad. Las prácticas no pretenden ser normas obligatorias de la industria, sino que sirvan como ejemplos específicos que se calibran en función de los riesgos, el contexto de la industria, el modelo comercial, el tamaño y el nivel de madurez de las organizaciones.

ELEMENTO DE RESPONSABILIDAD	PRÁCTICAS RELACIONADAS
Liderazgo y supervisión	• Compromiso y tono públicos desde arriba para respetar la ética, los valores y los principios específicos en el desarrollo, despliegue y uso de la IA. • Procesos institucionalizados de IA y toma de decisiones con criterios de escala. • Juntas, comités (internos o externos) de IA, ética, supervisión: para revisar los casos de uso de riesgo de la IA y mejorar continuamente las prácticas de IA. • Designación de un miembro del consejo para la supervisión de la IA. • Designación de un responsable de IA, un funcionario de IA o un líder de IA. • Creación de un consejo o comité interno interdisciplinar de IA. • Garantía de la inclusión y la diversidad en el desarrollo de modelos de IA y en los equipos de productos de IA.
Evaluación de riesgos	• Herramientas de evaluación del impacto algorítmico o de evaluación de la equidad para supervisar y probar continuamente los algoritmos con el fin de evitar prejuicios humanos, discriminación injusta y derivación conceptual a lo largo de todo el ciclo de vida de la IA. • Evaluación de la repercusión ética, sobre los derechos humanos y sobre la protección de datos. • Desarrollo de metodologías estandarizadas de evaluación de riesgos, que tengan en cuenta los beneficios y la probabilidad y gravedad de los factores de riesgo para las personas o la sociedad, el nivel de supervisión humana involucrado en las decisiones automatizadas individuales con efectos legales, así como su capacidad de explicación según el contexto y la posibilidad de auditoría. • Documentación de compensaciones (p. ej., exactitud —minimización de datos y seguridad—, transparencia, impacto sobre pocos beneficio para la sociedad) para el tratamiento de alto riesgo como parte de la evaluación de riesgos. • Evaluación de la calidad de los datos mediante el indicador clave de rendimiento (key performance indicator, KPI). • Evaluación de los datos en función de su finalidad: calidad, procedencia, personales o no, sintéticos, internos o de fuentes externas. • Marco para la preparación de datos y la evaluación de modelos, lo que incluye ingeniería de características, validación cruzada, pruebas retrospectivas y KPI validados por negocio. • Trabajar en estrecha colaboración entre el negocio y los expertos en datos (analistas de datos, ingenieros de datos, informáticos e ingenieros de programas informáticos) para evaluar periódicamente las necesidades y la precisión de los resultados con el fin de garantizar que el modelo pueda utilizarse correctamente.
Políticas y procedimientos	• Adoptar políticas y procedimientos específicos sobre cómo diseñar, utilizar o vender la IA. • Políticas sobre la aplicación de la privacidad y la seguridad por diseño en el ciclo de vida de la IA. • Regla que establece el nivel de verificación de la entrada y salida de datos. • Pruebas piloto de modelos de IA antes de su lanzamiento. • Uso de datos protegidos (p. ej., cifrados, medio anónimos, por medio de tókenes o sintéticos) en algunos modelos. • Uso de conjuntos de datos de alta calidad, pero más pequeños. • Uso de modelos de aprendizaje de IA federados, teniendo en cuenta la compensación con la seguridad de los datos y las responsabilidades de los usuarios. • Consideraciones especiales para las organizaciones que crean y venden modelos, programas

	informáticos y aplicaciones de IA. • Listas de comprobación o herramientas de diligencia debida y autoevaluación para socios comerciales que utilicen IA. • Definición de los pasos a seguir en materia de información, gobernanza y análisis de riesgos.
	• Fase de ideación entre todas las partes interesadas (científicos de datos, empresa, usuario final, funciones de control) en la que se debaten las necesidades, los resultados, las reglas de validación, el mantenimiento, la necesidad de capacidad de explicación y el presupuesto.
Transparencia	• Diferentes necesidades de transparencia para las personas, los reguladores, los socios comerciales y a nivel interno en las distintas fases del ciclo de vida de la IA en función del contexto. • Información adecuada comunicada de forma sencilla y fácil de entender. • Tener en cuenta que la IA debe ser inclusiva y accesible para las personas con necesidades especiales o discapacidades. • Establecer una pista de transparencia para propiciar la capacidad de explicación de las decisiones y el funcionamiento general del algoritmo para que el sistema de IA se pueda auditar. • Explicar que se trata de una decisión AI/ML, si hay posibilidad de confusión (prueba de Turing). • Proporcionar información de contraste. • Comprender las expectativas de los clientes y desplegar en función de su disposición a adoptar la IA. • Implementar la transparencia por niveles. • De la caja negra a la caja de cristal: análisis de los datos y del algoritmo/modelo. • Aspirar a la capacidad de explicación ayuda a entender la caja negra y genera confianza. • Definir criterios de despliegue de las tecnologías de IA en la organización basados en escenarios de uso y comunicarlos al usuario. • Elaborar fichas de modelos (documentos breves que acompañan los modelos de IA para describir el contexto en el que debe utilizarse el modelo, cuál es el procedimiento de evaluación). • Centro de datos para la transparencia en la gobernanza, accesibilidad, linaje, modificación y calidad de datos, definición, etc. • Adaptar la transparencia al riesgo identificado: p. ej., marca de agua para los resultados de la IA generativa.
Preparación y sensibilización	• Formación de científicos de datos, incluida la forma de limitar y abordar prejuicios. • Formación transversal: profesionales de la privacidad e ingenieros. • Formación en ética y equidad para los equipos tecnológicos. • Casos de uso en los que se ha detenido el despliegue problemático de la IA. • Función de los "traductores" en las organizaciones, para explicar la repercusión y el funcionamiento de la IA.
Control y verificación	• Capacidad de intervención humana en el diseño, la supervisión y la rectificación. • Capacidad de comprensión humana del negocio y los procesos mediante IA. • Capacidad de auditoría humana de las entradas y salidas. • Capacidad de revisión humana de decisiones individuales con efectos legales. • Supervisión del ecosistema desde el flujo de datos de entrada, el proceso de datos y el flujo de datos de salida. • Uso de diferentes técnicas de auditoría. • Confianza en las técnicas de pruebas de contraste. • Definición previa de los controles de auditoría de la IA. • Equipo de auditoría interna especializado en IA y otras tecnologías emergentes. • Los procesos deben permitir el control o la intervención humana en el sistema de IA cuando sea técnicamente posible y razonablemente necesario. • Seguimiento del modelo (validación cruzada y bucle de retroalimentación) y proceso de mantenimiento.
Respuesta y cumplimiento	• Procesos y procedimientos para recibir y abordar los comentarios y reclamos. • Mecanismos de recurso para subsanar una decisión de IA. • Rectificación de un humano, no de un robot. • Canal de retroalimentación.

[i] Para este informe, el Centre for Information Policy Leadership - CIPL utiliza el término "inteligencia artificial" de forma coherente con la definición de "sistemas de IA" desarrollada por el Instituto Nacional de Normas y Tecnología (National Institute of Standards and Technology, NIST) de EE. UU. en su Marco de Gestión de Riesgos 1.0, adaptado de una definición comparable desarrollada por la Organización para la Cooperación y el Desarrollo Económico (Organisation for Economic Cooperation and Development, OECD): "Un sistema de IA [se denomina así] a un sistema de ingeniería o basado en máquinas que puede, para un conjunto determinado de objetivos, generar resultados como predicciones, recomendaciones o decisiones que influyen en entornos reales o virtuales. Los sistemas de IA están diseñados para funcionar con distintos niveles de autonomía". Consulte https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf.

[ii] Por ejemplo: Italian Data Protection Authority "Garante" ban on ChatGPT del 30 de marzo de 2023 disponible en https://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/9870832 ; European Data Protection Board (EDPB) creates task force on Chat GPT, disponible en https://edpb.europa.eu/news/news/2023/edpb-resolves-dispute-transfers-meta-and-creates-task-force-chat-gpt_en; UK Competition and Markets Authority launches initial review of artificial intelligence models, disponible en https://www.gov.uk/cma-cases/ai-foundation-models-initial-review; The Office of the Privacy Commissioner of Canada has launched an investigation into ChatGPT, disponible en https://www.priv.gc.ca/en/opc-news/news-and-announcements/2023/an_230404/; Joint statement on enforcement efforts against discrimination and bias in automated systems USA Consumer Financial Protection Bureau, Department of Justice's Civil Rights Division, Equal Employment Opportunity Commission and Federal Trade Commission disponible en https://www.ftc.gov/system/files/ftc_gov/pdf/EEOC-CRT-FTC-CFPB-AI-Joint-Statement%28final%29.pdf.

[iii] Según la OECD, se han diseñado más de 800 iniciativas y estrategias de políticas sobre IA en 69 países, territorios y la Unión Europea https://oecd.ai/en/dashboards/overview.

[iv] CIPL, "First Report: Artificial Intelligence and Data Protection in Tension", octubre de 2018, https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_first_ai_report_-_ai_and_data_protection_in_tension__2_.pdf; "Second Report: Hard Issues and Practical Solutions", febrero de 2020, https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_second_report_-_artificial_intelligence_and_data_protection_-_hard_issues_and_practical_solutions__27_de febrero de_2020_.pdf; "Artificial Intelligence and Data Protection: How the GDPR Regulates AI", marzo de 2020, https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl-hunton_andrews_kurth_legal_note_-_how_gdpr_regulates_ai__12_de marzo de_2020_.pdf.

[v] CIPL, "Response to NTIA Request for Comment on AI Accountability Policy", junio de 2023, https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_response_to_ntia_ai_accountability_policy_june2023.pdf; "CIPL's Top Ten Recommendations for Regulating AI in Brazil," octubre de 2022, https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/[es]_cipls_top_ten_recommendations_for_regulating_ai_in_brazil__4_de octubre de_2022_.pdf; "Response to UK DCMS Proposed Approach to Regulating AI", septiembre de 2022, https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_response_to_uk_dcms_proposed_approach_to_regulating_ai_23_09_22.pdf; "CIPL Response to the EU Commission's Consultation on the Draft AI Act", julio de 2021, https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_response_to_the_consultation_on_the_draft_ai_act__29_de julio de_2021_.pdf.

[vi] No existen definiciones universalmente aceptadas para los desarrolladores, los que se encargan del despliegue y usuarios de IA; de hecho, una taxonomía para 2023 elaborada conjuntamente por la Unión Europea (UE) y EE. UU. describía las definiciones de los encargados del despliegue, desarrolladores y usuarios como "pendientes" (consulte "EU-U.S. Terminology and Taxonomy for Artificial Intelligence: First Edition", https://www.nist.gov/system/files/documents/noindex/2023/05/31/WG1%20AI%20Taxonomy%20and%20Terminology%20Subgroup%20List%20of%20Terms.pdf). En este documento, utilizamos el término "desarrolladores" para referirnos a las partes que diseñan y construyen sistemas de IA, "encargados del despliegue" para referirnos a las partes que ponen dichos sistemas a disposición de los usuarios y "usuarios" para referirnos a los usuarios finales que operan dichos sistemas de forma continua. Una única entidad podría desempeñar cada una de estas funciones en distintos momentos o simultáneamente.

[vii] *K-Nearest Neighbors Algorithm*, IBM, disponible en https://www.ibm.com/uk-en/topics/knn#:~:text=Next%20steps-,K%2DNearest%20Neighbors%20Algorithm,of%20an%20individual%20data%20point.
[viii] *3 ways autonomous farming is driving a new era of agriculture*, World Economic Forum, 2022, disponible en: https://www.weforum.org/agenda/2022/01/autonomous-farming-tractors-agriculture/
[ix] CIPL, "Artificial Intelligence and Data Protection: How the GDPR Regulates AI," marzo de 2020, https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl-hunton_andrews_kurth_legal_note_-_how_gdpr_regulates_ai__12_march_2020_.pdf.
[x] Para obtener más información sobre la intersección entre la IA y la regulación de la protección de datos, consulte CIPL AI First Report - *Artificial Intelligence and Data Protection in Tension*; CIPL AI Second Report - *Hard Issues and Practical Solutions*; and CIPL/Hunton Andrews Kurth White Paper - *How the GDPR Regulates AI* – disponible aquí https://www.informationpolicycentre.com/ai-proiect.html.
[xi] Para obtener más información sobre este tema, consulte CIPL, "First Report: Artificial Intelligence and Data Protection in Tension," octubre de 2018, cipl_first_ai_report_-_ai_and_data_protection_in_tension__2_.pdf (informationpolicycentre.com), y CIPL, "Second Report: Hard Issues and Practical Solutions," febrero de 2020, AI Project - Centre for Information Policy Leadership (informationpolicycentre.com).
[xii] Ministerial Declaration The G7 Digital and Tech Ministers' Meeting 30 April 2023 (g7digital-tech-2023.go.jp)
[xiii] G7 Hiroshima AI Process: G7 Digital & Tech Ministers Statement", septiembre de 2023, consultado en 3e39b82d-464d-403a-b6cb-dc0e1bdec642-230906_Ministerial-clean-Draft-Hiroshima-Ministers-Statement68.pdf (politico.eu).
[xiv] Certification Working Group, "Unlocking the Power of AI – Steps for Effective Certification to Help Drive Innovation and Trust," junio de 2023, https://www.responsible.ai/post/white-paper-draft-from-the-certification-working-group.
[xv] Para obtener más información sobre la gobernanza en estos niveles de la pila tecnológica de la IA, consulte Microsoft, "Governing AI: A Blueprint for the Future", mayo de 2023, https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RW14Gtw.
[xvi] National Institute of Standards and Technology (NIST), "AI Risk Management Framework," https://www.nist.gov/itl/ai-risk-management-framework; Personal Data Protection Commission (PDPC), "Singapore's Approach to AI Governance," https://www.pdpc.gov.sg/Help-and-Resources/2020/01/Model-AI-Governance-Framework, CIPL, "Organizational Accountability," https://www.informationpolicycentre.com/organizational-accountability.html.
[xvii] Consulte el informe del CIPL sobre tecnologías de mejora de la privacidad (de próxima publicación, otoño de 2023).
[xviii] Incentivizing Accountability: How Data Protection Authorities and Law Makers Can Encourage Accountability, CIPL, 23 de julio de 2018 disponible en https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_accountability_paper_2_-_incentivising_accountability_-_how_data_protection_authorities_and_law_makers_can_encourage_accountability.pdf.
[xix] En el DRCF participan la Autoridad de Competencia y Mercados (Competition and Markets Authority, CMA), la Oficina del Comisionado de Información (Information Commissioner's Office, ICO), la Oficina de Comunicaciones (Ofcom) y la Autoridad de Conducta Financiera (Financial Conduct Authority, FCA). Consulte https://www.gov.uk/government/collections/the-digital-regulation-cooperation-forum. Para obtener más información sobre la corriente de trabajo sobre transparencia algorítmica del DRCF, consulte https://www.gov.uk/government/publications/transparency-in-the-procurement-of-algorithmic-systems-findings-from-our-workshops.
[xx] En los Países Bajos, la Autoridad de Consumidores y Mercados (Authority for Consumers and Markets, ACM), la Autoridad Neerlandesa de Protección de Datos (AP), la Autoridad Neerlandesa de Mercados Financieros (Authority for the Financial Markets, AFM) y la Autoridad Neerlandesa de Medios de Comunicación (CvdM) pusieron en marcha el Foro de Cooperación sobre Regulación Digital (SDT). Consulte https://www.acm.nl/en/about-acm/cooperation/national-cooperation/digital-regulation-cooperation-platform-sdt. El Centro de Competencia para la Regulación de Plataformas Digitales (PEReN) de Francia se creó bajo la autoridad de los Ministerios de Economía, Cultura y Tecnología Digital. Basada en su experiencia en ciencia de datos, es una fuente de conocimientos técnicos y apoyo a los reguladores digitales franceses. Consulte https://www.peren.gouv.fr/en/. El Foro de Reguladores de Plataformas Digitales de Australia reúne a la Comisión Australiana de Competencia y Consumo (Australian Competition and Consumer Commission, ACCC), la Autoridad Australiana de Comunicaciones

y Medios de Comunicación (Australian Communications and Media Authority, ACMA), el Comisionado de Seguridad Electrónica (eSafety) y la Oficina del Comisionado Australiano de Información (Office of the Australian Information Commissioner, OAIC). Consulte https://www.accc.gov.au/about-us/media/media-updates/communique-digital-platforms-regulators-forum. Irlanda creó la Red de Reguladores Económicos, que reúne a siete reguladores. Consulte https://www.econreg.ie/about/our-members/.

[xxi] Consulte Christopher Hodges y CIPL, "Organizational Accountability in Data Protection Enforcement", octubre de 2021, https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_white_paper_on_organizational_accountability_in_data_protection_enforcement_-_how_regulators_consider_accountability_in_their_enforcement_decisions_6_oct_2021_.pdf

[xxii] Consulte la ponencia del CIPL "Regulatory Sandboxes in Data Protection – Constructive Engagement and Innovative Regulation in Practice - 8 de marzo de 2019 https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_white_paper_on_regulatory_sandboxes_in_data_protectionconstructive_engagement_and_innovative_regulation_in_practice_8_march_2019_.pdf .

[xxiii] ICO Regulatory Sandbox https://ico.org.uk/for-organisations/regulatory-sandbox/.

[xxiv] IMDA Data Regulatory Sandbox, https://www.imda.gov.sg/how-we-can-help/data-innovation/data-regulatory-sandbox.

[xxv] Datatilsynet AI Regulatory Sandbox, disponible en https://www.datatilsynet.no/en/regulations-and-tools/sandbox-for-artificial-intelligence/.

[xxvi] Sandbox on privacy by design and by default in Artificial Intelligence projects, Columbian Superintendence of Industry and Commerce, disponible en https://globalprivacyassembly.org/wp-content/uploads/2021/07/B6.-SIC-Colombia-Sandbox-on-privacy-by-design-and-by-default-in-AI-projects.pdf

[xxvii] CNIL, “Digital health and EdTech: the CNIL publishes the results of its first ‘sandboxes’“, julio de 2023, https://www.cnil.fr/en/digital-health-and-edtech-cnil-publishes-results-its-first-sandboxes.

[xxviii] Al momento de redactar este informe, los encargados de elaborar las políticas de la UE aún no habían decidido si la creación de entornos aislados de IA por parte de los estados miembros sería voluntaria u obligatoria. Consulte Luca Bertuzzi, “EU Council sets path for innovation measures in AI Act’s Negotiations”, *Euractiv*, 10 de julio de 2023. https://www.euractiv.com/section/artificial-intelligence/news/eu-council-sets-path-for-innovation-measures-in-ai-acts-negotiations/. Consulte también “First Regulatory Sandbox on Artificial Intelligence Presented,” *Digibyte*, 27 de junio de 2022, https://digital-strategy.ec.europa.eu/en/news/first- regulatory-sandbox-artificial-intelligence-presented.

[xxix] Consulte "Introducing Open Loop, a global program bridging tech and policy innovation", disponible en https://ai.facebook.com/blog/introducing-open-loop-a-global-program-bridging-tech-and-policy-innovation /; AI Impact Assessment: A Policy Prototyping Experiment, https://papers.ssrn.com/sol3/Delivery.cfm/SSRN_ID3772500_code715910.pdf?abstractid=3772500&mirid=1; and https://openloop.org/programs/open-loop-eu-ai-act-program/.

[xxx] IMDA, “Policy Prototyping,” Policy Prototyping | IMDA - Infocomm Media Development Authority. Meta’s TTC Labs is a partner for IMDA’s program.

[xxxi] CIPL, "Ten Principles for a Revised US Privacy Framework", marzo de 2019, https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_principles_for_a_revised_us_privacy_framework.pdf.

[xxxii] CIPL, “International Data Flows: Cross Border Privacy Rules, Privacy Recognition for Processors, and Global CBPR and PRP: Frequently Asked Questions", junio de 2023, https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_cpbr_and_prp_faq_jun23.pdf.

[xxxiii] OCDE, "Recommendation of the Council on Artificial Intelligence", mayo de 2019, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449

[xxxiv] El Acuerdo de Asociación de Economía Digital (Digital Economic Partnership Agreement, DEPA) es un acuerdo entre Nueva Zelanda, Singapur y Chile. Consulte https://www.mfat.govt.nz/en/trade/free-trade-agreements/free-trade-agreements-in-force/digital-economy-partnership-agreement-depa/.

[xxxv] The Global Partnership on Artificial Intelligence, https://gpai.ai/.