ISSN: 2528-7761

ECUADOR Debate 120

Quito/Ecuador/Diciembre 2023

Desafíos contemporáneos globales

ECUADOR
Debate 120

Desafíos contemporáneos globales

caap

ISSN: 2528-7761

ECUADOR DEBATE
Diego Martín de Utreras N28-43 y Selva Alegre
Apartado Aéreo 17-15-173B, Quito-Ecuador
Telf: 2522763 - 2523262
E-mail: revistaec@caapecuador.org
www.caapecuador.org/revista-ecuador-debate

SUSCRIPCIONES
Valor anual, tres números:
Exterior: USD$. 51.00
Ecuador: USD$. 21.00
Ejemplar suelto exterior: USD$. 17.00
Ejemplar suelto Ecuador: USD$. 7.00

Portada y diagramación
David Paredes

Impresión
El Chasqui Ediciones

ÍNDICE

DEBATE AGRARIO

ANÁLISIS

RESEÑAS

Ecuador Debate • ISSN: 2528-7761 • CAAP.
N. 120, diciembre 2023 - marzo 2024 • p. 119 - 133.

Análisis de impacto de la inteligencia artificial en los derechos y libertades de las personas

Luis Enríquez Álvarez*

Mucho se habla hoy en día acerca de los impactos jurídicos de la inteligencia artificial, pero muy poco se ha discutido acerca de los mecanismos para poder medirlos. Los nacientes proyectos para regular la inteligencia artificial se fundamentan en una gestión de riesgos, una práctica incomprendida en el mundo jurídico, el cual tradicionalmente se ha caracterizado en una toma de decisiones basada en criterios subjetivos. Sin embargo, considerando que la tendencia general en las ramas pertenecientes al derecho de tecnologías de la información ha sido meta-regulatoria, son los desarrolladores de productos basados en inteligencia artificial los encomendados para implementar una gestión de riesgos para la protección de derechos y libertades de las personas naturales. Desafortunadamente, los resultados de estos tipos regulatorios en áreas como la ciberseguridad y la protección de datos personales nos han mostrado el estado inmaduro de gestión de riesgos existente, en donde el mundo jurídico comete concurrentemente el grave error de asumir que una gestión de riesgos funciona por defecto. Este artículo pretende mostrar las vulnerabilidades de la regulaciones de inteligencia artificial basadas en una gestión de riesgos, los desafíos de un nuevo sistema de conformidad jurídica basada en riesgos, y la situación en la región andina, en donde son aún casi inexistentes todos estos temas centrales de protección de los derechos de las personas naturales a la luz de la inteligencia artificial.

Introducción

La inteligencia artificial puede definirse como "the science of making machines do things that would require intelligence if done by men" (Minsky 1968). Este sentido de reproducir la inteligencia humana no es nada nuevo, sin embargo se ha vuelto mucho más accesible para los humanos comunes en las últimas décadas, y en especial gracias a la explosión comercial de la inteligencia artificial generativa en noviembre del 2022, con la apertura al público general de chatGPT (Michalon y Camacho-Zuñiga 2023). Sin embargo, lo que llamamos hoy inteligencia artificial se fundamenta en cuatro paradigmas: el aprendizaje automático supervisado, el aprendizaje automático no supervisado, el aprendizaje automático de refuerzo (Russell y Norvig 2010), y el aprendizaje automático profundo (LISA Lab 2015). En este contexto, los *Large Language Models (LLM)*

* Analista cuantitativo de riesgos jurídicos, docente en la Universidad de Lille y en la Universidad Andina Simón Bolívar.

(Agüera y Arcas 2022) utilizados en la inteligencia artificial generativa usan para su aprendizaje modelos de procesamiento de lenguaje natural, de reconocimiento de audio, modelos de redes neuronales, entre otros.

Sin embargo, cuando hablamos de regulaciones jurídicas de la inteligencia artificial, nos enfrentamos a un entorno regulatorio mucho más complejo que la práctica regulatoria tradicional, en donde las autoridades de control están obligadas a desarrollar nuevos mecanismos proactivos de supervisión y control, que van mucho más allá de los mecanismos reactivos a los que han estado acostumbradas en el pasado. Esto hace que las regulaciones de la inteligencia artificial estén fundamentadas en la gestión de riesgos, una ciencia que hasta hoy ha sido incomprendida por el mundo jurídico.

Para una mejor comprensión de este artículo, este ha sido dividido en cuatro secciones: el problema regulatorio, el problema de la gestión de riesgos, el problema de la conformidad en riesgos y el problema en la Comunidad Andina.

El problema regulatorio

Dado que hoy en día se habla mucho acerca de los impactos de la inteligencia artificial en los derechos de las personas naturales, es primordial considerar el modelo regulatorio que están siguiendo las nuevas regulaciones de la inteligencia artificial, el cual puede encuadrarse a la luz de la doctrina de la gobernanza corporativa. Desde finales del siglo XX, nuevos modelos de gobernanza corporativa fueron propuestos, saliendo de un esquema prescriptivo, hacia modelos regulatorios flexibles y responsivos. Un modelo prescriptivo es conocido como *command and control* (Parker 2022, 8), en el cual los regulados siguen al pie de la letra lo establecido por los reguladores, modelo aun presente en el derecho administrativo, pero muchas veces poco efectivo en temas digitales, por falta de comprensión del riesgo por parte de las autoridades reguladoras, con un efecto que puede culminar en un ejercicio de *compliance en papel. Al otro extremo de las regulaciones tipo command and control tenemos como alternativa a la auto-regulación* (Parker 2022, 136), modelo mediante el cual son los regulados quienes deciden sus estándares de gobernanza de procesos y manejo de riesgos. Sin embargo, la auto-regulación ha mostrado otro gran problema, la falta de compromiso de los regulados para proteger algo más allá que sus propios intereses económicos (Parker 2022).

En el medio de ambos modelos surgieron varias alternativas que pueden ser viables para la regulación de la inteligencia artificial. Ayres y Braithwaite (1992, 101) propusieron el concepto de *enforced self-regulation*, como una alternativa

mediante la cual los reguladores se convierten en supervisores de los procesos auto regulatorios de los regulados. Esta proposición evolucionó hacia el concepto de meta-regulación propuesto por autores como Grabosky (2017, 149) y Parker (2022, 245), el cual consiste en la regulación de los reguladores acerca de la auto-autoregulación de los regulados. El concepto de meta-regulación ha sido ampliamente difundido en áreas en las cuales la inteligencia artificial tiene dependencias, tales como las regulaciones jurídicas de protección de datos personales y las regulaciones jurídicas de ciberseguridad. Una meta-regulación es muy compatible a la vez con el concepto de regulaciones basadas en riesgos, en cuanto el derecho regulatorio delega a las instituciones públicas o privadas a gestionar los riesgos propios de las actividades reguladas, como sucede tradicionalmente en el ámbito financiero, ambiental, o de la salud.[1]

En este contexto, una meta-regulación puede ser muy bien justificada en el ámbito de la inteligencia artificial, por cuanto la autoridad de control podría no tener el mismo nivel de conocimiento que las empresas reguladas acerca de gestionar los riesgos de esta. Sin embargo, en un entorno meta-regulatorio, el rol del regulador es fundamental para lograr una alta efectividad en la protección de los derechos y libertades de los ciudadanos. En este contexto, Sparrow (2000) identificó los problemas que pueden presentarse a nivel del derecho regulatorio y la importancia de la gestión de riesgos en la práctica regulatoria.[2] Desde el enfoque de esta área del derecho, una mala comprensión acerca de los mecanismos utilizados para medir riesgos puede conllevar al fracaso de las futuras regulaciones de la inteligencia artificial. Por ejemplo, utilizar matrices de riesgo con escalas subjetivas, con etiquetas de bajo riesgo o alto riesgo, sin ninguna justificación científica, puede conllevar a un caos interpretativo, como ya ha pasado en otras regulaciones digitales.[3] Desde el enfoque de la práctica regulatoria, en cambio, la gestión de riesgos presenta muchas ventajas a nivel estratégico que las autoridades controladoras muy bien pueden aprovechar.

En este contexto, bien cabe referirse a la importancia de encomendar la gestión de riesgos a los regulados sin mayores detalles, pero trabajar en estrategias de permeabilidad (Parker 2022, 197), promoviendo una adecuada gestión de riesgos

1 Por ejemplo, la Directiva establece el análisis cuantitativo certificado de actuarios en el área de los fondos de pensiones. Ver: UE 2016b, art 13s.

2 Para Sparrow (2000, 27), "laws are often out of date. Therefore should ignore those that are obsolete or unimportant and should take the initiative in tacking emerging issues and risks, even before they are recognized in law, building public support as they go".

3 Hay muchos problemas con métodos tradicionales como las matrices de riesgos, que deben ser remplazados por otros más objetivos y confiables. Ver: Cox (2008, 501).

de la inteligencia artificial basada en modelos de riesgos y métricas significativas, desde el derecho secundario. No obstante, las autoridades de control deben considerar que también precisan entrar en un proceso de transformación hacia una cultura del riesgo, dejando atrás las malas prácticas de gestión basadas únicamente en análisis cualitativos, y transformarse hacia una cultura de medición del riesgo a través del análisis cuantitativo. Todo esto, considerando que las autoridades de control también tienen un presupuesto limitado y necesitan gestionarlo de manera eficiente hacia estrategias proactivas de identificación y monitoreo de inconformidades a las regulaciones de la inteligencia artificial, y no únicamente a través de estrategias reactivas sancionadoras (Sparrow 2000, 265-266). Desde esta perspectiva, el motivo principal de un cambio estratégico hacia la práctica regulatoria proactiva cobra enorme importancia, considerando los potenciales riesgos jurídicos que conlleva la inteligencia artificial.

En consecuencia, la primera regulación jurídica de la inteligencia artificial que tendrá un impacto global es la propuesta sobre la *Artificial Intelligence Act*, que será aprobada en la Unión Europea a fines del 2023 y entraría en aplicación en el 2026 (European Commission 2021). Esta regulación es en esencia una meta-regulación y una regulación fundamentada en riesgos. Su alcance territorial sobrepasa las fronteras de la Unión Europea por cuanto incluso deben conformase "los proveedores y usuarios de sistemas de IA que se encuentren en un tercer país, cuando la información de salida generada por el sistema se utilice en la Unión" (European Commission 2021, art 2). La regulación exige un análisis de conformidad y una documentación técnica, la cual se debe fundamentar en la gestión de riesgos acerca de la robustez y la ética de los algoritmos, pero a la vez depende de una gestión de riesgos[4] holística que incluya a la protección de datos personales (art 10) y a la ciberseguridad (art 15), para lograr su propósito de protección a los derechos fundamentales de las personas naturales.

El problema del riesgo

La falta de definición acerca de lo que es un riesgo, y definir una clara perspectiva para la gestión del riesgo, ha sido una constante en el mundo jurídico. Así vemos como muy relevantes regulaciones en el entorno digital, tales como el Reglamento General de Protección de Datos –RGPD– (UE 2016a) o la misma *Artificial*

4 "El sistema de gestión de riesgos consistirá en un proceso iterativo continuo que se llevará a cabo durante todo el ciclo de vida de un sistema de IA de alto riesgo, el cual requerirá actualizaciones sistemáticas periódicas" (European Commission 2021, art 9).

Intelligence Act, no incluyen estas definiciones fundamentales en sus glosarios. El proceso de elaboración del RGPD tuvo varios debates al respecto, que simplemente mostraron un muy bajo nivel comprensión de lo que es una gestión de riesgos por parte del mundo jurídico. El *Article 29 Working Party* estableció en el contexto del RGPD:

> ...even with the adoption of a risk-based approach – there is no question of the rights of individuals being weakened in respect of their personal data. Those rights must be just as strong even if the processing in question is relatively low risk (Art.29WP 2014, 2).

Con ello, el riesgo se convirtió en el corazón mismo del RGPD, pero con una inmensa limitación metodológica, los regulados y los reguladores tenían poco conocimiento de lo que era este nuevo tipo de gestión de riesgos fundamentada en la protección de los derechos y libertades de las personas naturales (UE 2016a, art 32). Una similar situación se puede apreciar en el Ecuador de hoy, con la entrada en aplicación de la Ley Orgánica de Protección de Datos Personales,[5] la cual heredó las mismas carencias del RGPD y en donde casi todos quienes venden servicios de gestión de riesgos están simplemente desorientados. La International Standards Organization (ISO) define al riesgo como un "effect of uncertainty on objectives",[6] con una visión de ganancia o pérdida. Para Hubbard (2020, 110), el riesgo es "a state of uncertainty where some of the possibilities involve a loss, injury, catastrophe, or other undesirable outcomes", una visión cuantitativa que se alinea muy bien a la necesidad de comprensión de la situación del riesgo actual de los sistemas basados en inteligencia artificial, los cuales amenazan varios derechos y libertades de las personas naturales.

La realidad es que, debido a la ausencia de una rama propia de gestión de riesgos de protección de datos personales, lo que se ha hecho es mezclar dos visiones antagónicas de manejo de riesgos, que requieren de una personalización para funcionar juntas, combinando el enfoque jurídico y el enfoque científico. Para Hubbard, existen cuatro visiones de manejos de riesgos en el mundo contemporáneo: "the actuaries, the war quants, the economists, and the management consultants" (2020, 82-83). Las tres primeras pertenecen a una visión del riesgo científica, en la cual deben medirse la probabilidad de ocurrencia y el impacto, con justificaciones

5 Ver artículo 37 de la Ley Orgánica de Protección de Datos Personales. 2021, de 10 de mayo. Registro Oficial, Asamblea Nacional de la República del Ecuador. Año II, nº 479, Quito, 26 de mayo de 2021. https://n9.cl/mv7ow.

6 ISO/IEC 27000:2018, clause 3.61.

racionales casi siempre cuantitativas. Sin embargo, la cuarta categoría de *consultores* ha sido la utilizada mayormente en la industria de la ciberseguridad, la cual se ha caracterizado más bien por utilizar metodologías de estándares de organizaciones internacionales con supuestas mejores prácticas, que a la final han sido malinterpretadas por la industria, por cuanto son normas encaminadas a la gobernanza de procesos y gestión de proyectos, y no a la medición de riesgos.[7]

Como ejemplo, la gestión riesgos de protección de datos personales es muy malentendida en la actualidad, lo cual se refleja en una dudosa efectividad de control regulatorio. Por un lado, es aún incomprendida la interdependencia entre los riesgos de seguridad de datos personales y los riesgos de conformidad jurídica, lo cual es muy confuso para responsables del tratamiento, quienes piensan que lo necesario es seguir únicamente guías de buenas prácticas que a veces tienen vacíos en cuanto a conceptos básicos del riesgo.[8] Por otro lado, las agencias regulatorias promueven metodologías de gestión de riesgos con enormes carencias, fundamentadas únicamente en el análisis cualitativo de riesgos, y una visión taxonómica de medidas de seguridad organizacionales y técnicas, tal como si fuese un catálogo. Para entender mejor esta errónea visión de una gestión de riesgos, podemos pensar en un paciente que acude a un médico en razón de un dolor en el estómago y que el médico le envíe antibióticos o lo lleve al quirófano de manera directa, en lugar de realizar previamente análisis cuantitativos tales como los exámenes de sangre. Este ejemplo representa claramente el dilema del riesgo regulatorio, y la necesidad de una transformación tanto de reguladores como de regulados. En este contexto, estándares de buenas prácticas tales como el ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27005, ISO/IEC 31000, el Cobit 5, el NIST SP800-30, pueden ser útiles para la gestión de proyectos de implementación, pero son incompletos si no se adopta una adecuada gestión fundamentada en modelos de riesgo adecuados, métricas significativas, comparaciones efectivas, con el fin de tomar decisiones informadas (Freund y Jones 2015, 279). En pocas palabras, estos estándares solo son guías, que requieren ser complementados desde una perspectiva científica, racional y efectiva acerca del manejo de riesgos.

7 En este contexto, el único estándar ISO/IEC de la serie 27000, es el ISO/IEC 27004, el cual únicamente provee criterios de medición, pero no calibración de métricas cuantitativas ni modelos de riesgos.

8 Por citar un ejemplo, el estándar ISO/IEC 29134:2017 promovía una guía para realizar *Privacy Impact Assessments*, que omitía básicos principios de una gestión de riesgos, tales como medir la probabilidad de ocurrencia en un lapso de tiempo determinado, o respaldar las escalas cualitativas de riesgos con cifras cuantitativas. La nueva versión 2023 ha enmendado varias falencias de la versión anterior. Ver: ISO/IEC 29134:2017, e ISO/IEC 29134:2023.

En este contexto, tenemos que comprender, por un lado, que la gestión de riesgos de ciberseguridad se encuentra aún en una etapa inmadura, la cual ha empezado a transformarse recién en la última década. Es así que el Foro Económico Mundial (2015, 3) tuvo la iniciativa de promover la adopción de una gestión cuantitativa de riesgos de ciberseguridad con su iniciativa "Partnering for Cyber Resilience Towards the Quantification of Cyber Threats", en el año 2015. Sin embargo, esto no es aún el estado del arte en la ciberseguridad, y así como la protección de datos personales heredó una gestión de riegos inmadura, la inteligencia artificial corre el grave riesgo de repetir el mismo error. Por otro lado, la gestión de riesgos jurídicos de la inteligencia artificial replica los análisis de impacto, ya utilizados en otras áreas, pero muy probablemente con una considerable influencia de los análisis de impacto encontrados en las regulaciones de privacidad y protección de datos personales. En este contexto, los Privacy Impact Assessments (PIA), heredaron una visión superficial de manejo de riesgos fruto de los Fair Information Practice Principles (FIPPs) en 1973 (Shapiro 2021, 21), y muy poco han cambiado con el tiempo. Para Shapiro, el primer error principal de los PIA es que "PIAs tend to emphasize description over analysis, which prejudices them toward addressing privacy in a checklist fashion"; es decir, son listas subjetivas de chequeo. El segundo error consiste en que "even when PIAs do explicitly invite discussion of possible privacy risks and potential mitigation strategies, risks are typically construed narrowly" (Shapiro 2021), lo cual significa que en la práctica se interpretan de manera separada a otros ámbitos del riesgo, como la ciberseguridad y las finanzas. El gran problema de la gestión de riesgos para la protección de derechos y libertades de las personas naturales es la falta mecanismos cuantitativos para medir el impacto que puede tener una violación de datos o errores de funcionamiento, en sus derechos. La gran paradoja es que mientras relevantes autores jurídicos concuerdan en la importancia de mejorar la gestión de riesgos, al mismo tiempo algunos se oponen a la medición cuantitativa de tales impactos por cuanto serían muy subjetivos e inciertos, a pesar de ser justamente esa la finalidad de una gestión de riesgos, pues si no hubiese incertitud ésta no sería necesaria.

En este contexto cabe recordarnos que medir riesgos no es nada nuevo en otras áreas de estudio, y que los actuarios lo hacen desde hace alrededor de doscientos años (SOA 2008, 3), en donde su profesión fue creada ante a la necesidad de medir los riesgos relacionados a las pensiones de retiro, tal como hoy es necesario para áreas como la protección de datos personales y la inteligencia artificial. Negar la posibilidad de medir el impacto de la inteligencia artificial en

los derechos y libertades de las personas naturales de manera cuantitativa equivale a, desde ya, condenar las nuevas regulaciones de inteligencia artificial hacia un fracaso eminente.

El problema de la conformidad en riesgos

Es cotidiano escuchar al mundo de las ciencias sociales hablar de manera empírica acerca del impacto de la inteligencia artificial en áreas como la generación de empleo, la vida privada, la justicia, entre otras. Sin embargo, estos riesgos solamente pueden ser encuadrados a la luz de la normativa jurídica y no de la ética. Es así que el impacto laboral de la pérdida de empleos requiere de algún tipo de regulación jurídica que pueda actuar como medida de control de riesgos en este ámbito, como por ejemplo, regular acerca del balance entre humanos y agentes inteligentes, el régimen fiscal de la inteligencia artificial,[9] u otras medidas compensatorias para este tipo de impacto laboral. Sin embargo, la inteligencia artificial puede también violar derechos de manera directa tales como el derecho a la protección de datos personales, el derecho a la imagen, e incluso el derecho a la vida. En este contexto, las regulaciones jurídicas de la inteligencia artificial tienen como posibilidad pedir de manera obligatoria a los desarrolladores y vendedores de productos de inteligencia artificial el realizar un análisis de impacto que pueda mostrar una pragmática disminución de los niveles de riesgos en tales productos. Ante ello, el concepto de *risk-based accountability* (Gellert 2020, 152) debe ser entendido a profundidad, por cuanto transforma una visión de conformidad legal binaria –cumple o no cumple– hacia una visión probabilística de la conformidad legal. Para Gellert (2020), refiriéndose al RGPD, "risk management is at the heart of the accountability principle and of risk-based approach". En consecuencia, un derecho no puede ser protegido al cien por ciento, pues el riesgo es medido de manera probabilística, lo cual bien puede contradecir los tradicionales postulados del derecho. Las nuevas regulaciones de inteligencia artificial vienen impregnadas de este tipo de conformidad en riesgos, y desde ya existen metodologías para lograrlo.

La ISO publicó el estándar ISO/IEC 23894:2023 con una visión de riesgos que sigue su linaje de guías para la gestión de riesgos que inició con el célebre ISO 27005:2022, fundamentado en el establecimiento del contexto, identificación, análisis, evaluación, y tratamiento de riesgos, brindando un aporte limitado

9 Ver entrevista a Bill Gates en Murayama 2018.

en el tema. El NIST, por su parte, publicó el NIST AI 100-1, una guía para los riesgos de la inteligencia artificial más completa,[10] pero que tampoco resuelve el problema principal, obtener métricas para una adecuada gestión cuantitativa de riesgos de la inteligencia artificial. Una metodología más específica es el cap AI (Floridi et al. 2021), desarrollado por la Universidad de Oxford, el cual presenta una perspectiva de análisis cuantitativo mucho más adecuada para los análisis de conformidad para la Artificial Intelligence Act, el cual se fundamenta en dos grandes grupos de métricas, el primero para medir la *robustez*,[11] y segundo para la *equidad*[12] de un producto o servicio basado en inteligencia artificial.

En este contexto, las métricas casi exclusivamente hacen referencia más bien a la robustez operacional de los algoritmos, están encaminadas hacia un funcionamiento de buen desempeño probabilístico que minimice los riesgos de mal funcionamiento y errores. Ejemplos de métricas para la robustez son "Mean Square Error, Mean Absolute Error, Accuracy" (Floridi et al. 2021, 36-37), entre otras. La robustez puede ser asociada también a escenarios de gestión de riesgos de ciberseguridad, tales como la seguridad física del producto, en caso de *alucinaciones de la inteligencia artificial*, o escenarios de ciberataques, tales como el *envenenamiento de datos* en un contexto de *adversarial machine learning* (European Commission et al. 2023, 7). Por otro lado, ejemplos de métricas para la equidad son: "Statistical Parity Difference, Theil Index, Equal Opportunity" (European Commission et al. 2023, 50-51), entre otras. Este tipo de métricas consiste en la no discriminación de un sistema de inteligencia artificial de los derechos y libertades de las personas físicas. Si bien es cierto que medir la equidad es algo controversial, pues parece ser un tema subjetivo que ya conocimos en el área de la protección de datos personales, otras soluciones han emergido y están en este momento discutiéndose en las comunidades académicas para una mejor estimación. Entre ellas, la proposición de la multidimensionalidad del riesgo de la inteligencia artificial y el uso de la analítica legal para más bien analizar el razonamiento legal de las autoridades sancionadoras, lo cual sin duda puede dar enormes luces a las instituciones públicas y privadas que deben buscar la conformidad legal con las nuevas regulaciones de inteligencia artificial (Enríquez 2023, 27).

10 "*AI risks or failures* that are not well-defined or adequately understood are difficult to measure quantitatively or qualitatively". NIST AI 100-1, cláusula 1.21.

11 "Some typical issues include overfitting/underfitting, bugs, validation issues and data issues" (Floridi et al. 2021, 49).

12 "In order to choose from multiple strategies to avoid discrimination, developers first need to define and operationalise model 'fairness' based on the context and use case" (Floridi et al. 2021, 49).

Dado que para modelar riesgos es necesario incluir estos aspectos de robustez y equidad de la inteligencia artificial en escenarios reales de riesgos, un ejemplo es el *Factor Analysis of Information Risk, conocido como modelo FAIR* (O'Reilly 2019), que ha sido uno de los factores transformadores en la industria de la ciberseguridad en la última década, y que ha influido en otras áreas del riesgo operacional. Otras investigaciones, muestran que puede ser también utilizado en el área de la privacidad y la protección de datos (Cronk y Shapiro 2021, 346). El modelo propone conceptos fundamentales del riesgo, como medir las probabilidades de ocurrencia en un lapso de tiempo determinado o una visión multidimensional del impacto, clasificándolo en pérdidas primarias y secundarias (Freund y Jones 2015, 66-73). Sin embargo, todo lo aquí propuesto no será posible si no adoptamos una visión cuantitativa de los análisis de impacto. Curiosamente, esto es algo que la inteligencia artificial generativa aún no puede responder, por cuanto no hay una solución definitiva en el horizonte.

El problema de la Comunidad Andina

En la Comunidad Andina de Naciones (CAN) aún no se ha analizado el problema planteado en este artículo. En este contexto, podemos ver un gran retraso en temas regulatorios sobre nuevas tecnologías en relación a otras regiones del mundo, y particularmente la Unión Europea. Sin embargo, los primeros esfuerzos han salido a la luz, siendo Colombia el país andino que ya ha propuesto una "Política nacional para la transformación digital e inteligencia artificial" (Conpes 2019), aunque fuera del contexto jurídico de la CAN. Estas propuestas, en el ámbito de las políticas públicas, dependen en gran medida de dar un salto desde la teoría a la práctica. Así podemos notar en el Ecuador que iniciativas como la transición hacia una *economía social del conocimiento* (Vila-Viñas y Barandiaran 2015) o el *Libro Blanco de la sociedad de la información de la sociedad de la información y del conocimiento* (Mintel 2018) "sólo han vendido humo", y han fracasado por cuanto no abordan los problemas de fondo de nuestros países, existiendo aún otros problemas previos que deben ser resueltos, tales como la conectividad y las brechas digitales.

Desde una perspectiva normativa, en otras áreas del derecho digital, podemos observar una gran disparidad entre los países de la Región Andina, en temas como la protección de datos personales; siendo esta un área jurídica de la cual depende la inteligencia artificial. Bolivia ni siquiera tiene aún una ley de protec-

ción de datos y el Ecuador, a pesar de tener una,[13] hasta noviembre del 2023 no ha establecido una autoridad de protección de datos, muy probablemente por la indiferencia del último gobierno hacia el tema. Además, podemos también considerar en esta área que Perú y Colombia publicaron sus respectivas leyes de protección de datos recién en los años 2011 y 2012,[14] respectivamente, y más bien sincronizadas con la Directiva Europea del año 1995. Considerando que la propuesta del RGPD nace en enero del 2012 (European Commission 2012), podemos constatar que incluso los países más rápidos en regular asuntos digitales, están usualmente rezagados. En materia de riegos de ciberseguridad tampoco hay normativa comunitaria relevante, y el proyecto de ley de seguridad digital que ha sido propuesto en el Ecuador no está centrado sobre la gestión cuantitativa de riesgos como tal, muy probablemente replicando los mismos errores de una gestión de riesgos superficial (Asamblea Nacional 2023).

Esto nos da la pauta de un retraso normativo considerable de los países andinos, con un mundo que se intenta ya acoplar a una cuarta revolución industrial, condenando nuevamente a la región a un atraso productivo, a un atraso normativo, y muy probablemente a un atraso educativo que solo está formando consumidores de tecnología y no desarrolladores, innovadores, ni emprendedores. Todo esto con la consideración especial de que las empresas utilizan sistemas inteligentes para sus procesos empresariales, los gobiernos utilizan de manera empírica sistemas de inteligencia artificial en áreas como la vigilancia y reconocimiento facial, y las personas naturales están totalmente desprotegidas por este enorme vacío legal.

Analizar los factores para este retraso regulatorio permite apreciar que pueden deberse a muchas causas sobre las que no vale la pena elucubrar, pero es conveniente aprender de las experiencias de las regulaciones de inteligencia artificial en otras regiones del mundo, para así lograr una efectiva transformación basada en la gestión de riesgos. El objetivo de tal transformación digital hacia la inteligencia artificial debe ser medible, para mejorar la administración pública y hacer más competitivas a las empresas privadas andinas. Ante ello sería muy interesante analizar el estado de la gestión de los riesgos en nuestros países, el cual en estas áreas sigue siendo eminentemente cualitativo. Es muy importante poner la casa en orden, priorizando la disminución inmediata de la

13 Ver: Ley Orgánica de Protección de Datos Personales. Quinto Suplemento del Registro Oficial No.459 , 26 de Mayo 2021.

14 Ley N.° 29733 (Perú), de Protección de Datos Personales y Ley Estatutaria 1581 (Colombia), por la cual se dictan disposiciones generales para la protección de datos personales.

brecha digital en el acceso, así como, luchar por disminuir la brecha existente en la educación digital, lo cual incluye una considerable transformación del sistema educativo. La consecuencia de no hacerlo es perder una oportunidad importante e irrepetible en el contexto de la economía digital, en donde necesitamos investigación científica, investigación jurídica y transitar hacia una transformación eficaz de las regulaciones jurídicas basadas en riesgos, la de una cultura de medición del riesgo.

Conclusión

Este artículo ha abordado el análisis de impacto de la inteligencia artificial, enfocándose en la necesidad de cambiar nuestra concepción sobre la conformidad en riesgos. Para ello, es necesario considerar tres problemas contemporáneos: los problemas regulatorios, los problemas del riesgo, y los problemas de la conformidad en riesgos. La conclusión principal es que los modelos meta-regulatorios fundamentados en riesgos lamentablemente se ven amenazados por una incomprensión del mundo jurídico acerca de lo que realmente es una gestión de riesgos. Ante ello, el estado actual del riesgo operacional es inmaduro, y el estado actual de la gestión de riesgos jurídicos esta recién naciendo.

Como alternativa, la noción de *risk-based compliance* debe ser mejor entendida por las instituciones privadas y públicas, pero también por los reguladores, quienes incluso en países de alto desarrollo tecnológico han demostrado que su nivel de comprensión del riesgo es deficiente. Recordemos que las nuevas legislaciones de la inteligencia artificial deben cumplir con la complicada misión de vigilar las gestiones de riesgos de instituciones privadas y públicas de manera proactiva. Finalmente, no hay mucho que decir aún de la Comunidad Andina en el área de los riesgos de la inteligencia artificial, pero sí que sería recomendable que en ella también se empiece un proceso de actualización acerca del riesgo regulatorio y, sobre todo, sobre su rol para poder controlar de manera proactiva los riesgos que presenta la inteligencia artificial contra los derechos y libertades de los ciudadanos. En este contexto, los efectos de la inteligencia artificial en nuestra población son evidentes, pues son tecnologías disruptivas abiertas para todos, sea cual sea el nivel de educación digital que el usuario tenga. En el ámbito regulatorio, la situación actual en los países de la Comunidad Andina es una completa desconexión de parte de los legisladores con respecto a los enormes cambios globales que afectan también de manera directa a nuestros ciudadanos y nuestras sociedades.

Debemos empezar a cuestionarnos acerca de las consecuencias que la desregulación de la inteligencia artificial tendrá en nuestros sistemas democráticos, en donde el perfilamiento de la gobernanza algorítmica afecta de manera directa derechos fundamentales como la libertad de expresión, con un efecto contrario al esperado, pues las personas empiezan a recibir información únicamente de acuerdo a sus preferencias, lejos de la neutralidad esperada a la luz de este derecho. A la vez, las enormes deficiencias en educación digital de nuestros sistemas educativos aumentan la probabilidad de ocurrencia de los riesgos asociados a la inteligencia artificial, ante la ausencia de controles de riesgo organizacionales y jurídicos. Es tiempo de entender que no se trata de ciencia ficción, ni de escenarios de riesgos futuros, sino más bien de una realidad actual contundente, irreversible y, a la vez, llena de incertidumbres.

Bibliografía

Agüera y Arcas, Blaise. 2022. Do Large Language Models Understand Us? Massachusets: MIT Press.

Asamblea Nacional. 2023. "El Proyecto de Ley de Seguridad Digital tiene informe favorable para primer debate en el pleno". Prensa, Asamblea Nacional, 22 de marzo. Quito, Ecuador.

Ayres, Ian y John Braithwaite. 1992. Responsive Regulation: Trascending the Deregulation Debate. Oxford: Oxford University Press. https://n9.cl/o0cmv1.

Cox, Anthony. 2008. "What's Wrong with Risk Matrices". Risk Analysis 28 (2): 497-512.

Conpes (Consejo Nacional de Política Económica y Social, República de Colombia). 2019. Política Nacional para la Transformación Digital e Inteligencia Artificial. Documento Conpes 3975. Departamento Nacional de Planeación, Ministerio de Tecnologías de la Información y las Comunicaciones. https://n9.cl/ogh3r.

Cronk, Jason y Stuart Shapiro. 2021. "Quantitative Privacy Risk Analysis". IEEE European Symposium on Security and Privacy Workshops (EuroS&PW 2021): 340-350. https://n9.cl/l6jto.

Enríquez, Luis. 2023. "Using the FAIR model for Risk-based Accountability". FAIRCON23 conference day 2, Video, 43:42. Washington D.C.: FAIR Institute. https://n9.cl/0ks0t .

European Commission. 2012. Proposal for a Regulation of the European Parliament and the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). Eur-Lex. Brussels. https://n9.cl/rgozk.

_____ 2021. Proposal for a Regulation of the European Parliament and of the Council laying down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending certain Union Legislative Acts. EUR-Lex. https://n9.cl/cqos34.

_____ 2014. Art.29WP (Article 29 Data Protection Working Party). 2014, May 30th. "Statement on the role of a risk-based approach in data protection legal frameworks". European Commission, Brussels. https://n9.cl/e2wiv.

European Commission, Joint Research Centre, Henrik Junklewitz, Ronan Hamon, Antoine-Alexandre André. 2023. *Cybersecurity of artificial intelligence in the AI Act – Guiding principles to address the cybersecurity requirement for high-riskAI systems, Publications Office of the European Union*. https://n9.cl/homqb.

Floridi, Luciano, Matthias Holweg, Mariarosaria Taddeo, et al. 2022. "capAI - A Procedure for Conducting Conformity Assessment of AI Systems in Line with the EU Artificial Intelligence Act". Available at SSRN: https://n9.cl/uk96b.

Foro Econónimo Mundial. 2015. *Partnering for Cyber Resilience Towards the Quantification of Cyber Threats*. WEF. https://n9.cl/jbtoe.

Freund, Jack y Jack Jones. 2015. *Measuring and Managing Information Risk: A FAIR Approach*. United States: Elsevier.

Grabosky, Peter. 2017. "Meta-Regulation". In *Regulatory Theory: Foundations and Applications*, edited by Peter Drahos, 149–62. ANU Press. https://n9.cl/c0j52.

Gellert, Raphaël. 2020. *The Risk-Based Approach to Data Protection*. Oxford: Oxford University Press.

Hubbard, Douglas. 2020. *The Failure of Risk Management*. United States: John Wiley.

LISA Lab. 2015. Deep Learning Tutorial. University of Montreal.

Michalon, Barthélémy & Claudia Camacho-Zuñiga. 2023. "ChatGPT, a brand-new tool to strengthen timeless competencies". *Frontiers in Education 8*. DOI: https://n9.cl/gn9ml.

Ministerio de Telecomunicaciones y de la Sociedad de la Información, República del Ecuador. 2018. *Libro Blanco de la Sociedad de la Información y del Conocimiento*. Quito: MINTEL. https://n9.cl/ap3dy.

Minsky, Marvin. 1968. *Semantics Information Processing*. Cambridge: MIT Press.

Murayama, Keiichi. 2018. "Interview: 'Robot taxes' will help keep humans employed, Bill Gates predicts". *Nikkei Asia*, 3 de noviembre. https://n9.cl/sg4ai.

O'Reilly, Paige. 2019. "The FAIR Model Explained in 90 Seconds". RiskLens [Blog], August 22. https://n9.cl/twl4e.

Parker, Christine. 2022. *The Open Corporation*. Melbourne: Cambridge University Press.

Russell, Stuart y Peter Norvig. 2010. *Artificial Intelligence A Modern Approach*. New Jersey: Pearson Education.

Shapiro, Stuart. 2021. "Time to Modernize Privacy Risk Assessment", *Issues in Science and Technology* 38 (1): 19-22.

SOA (Society of Actuaries). 2008. *Module 1: Role of the Professional Actuary*. Society of Actuaries.

Sparrow, Malcolm. 2000. *The Regulatory Craft*. Washington D.C.: Brookings Institution Press.

UE (Unión Europea). 2016a. Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo

que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE. EUR-Lex. https://n9.cl/ebg5j.

_____ 2016b. Directiva 2016/2341 del Parlamento Europeo y del Consejo, de 14 de diciembre de 2016, relativa a las actividades y la supervisión de los fondos de pensiones de empleo (FPE). EUR-Lex. https://n9.cl/bz88q.

Vila-Viñas, David y Xabier E. Barandiaran, eds. 2015. *Flok Society: Buen Conocer. Modelos sostenibles y políticas públicas para una economía social del conocimiento común y abierto en el Ecuador*. Quito: IAEN.