LA GOBERNANZA DE LOS DATOS DE LA SOBERANÍA TERRITORIAL A LA SOBERANÍA DIGITAL

Data governance from territorial sovereignty to digital sovereignty

Governação dos dados da soberania territorial à soberania digital

Yamila Eliana Juri
Universidad Nacional de Cuyo-Conicet y UNIVERSIDAD JUAN A. MAZA., Mendonza, Argentina
ORCID: https://orcid.org/0000-0002-3136-4144
E-mail: yamilajuri@gmail.com

Trabalho enviado em 11 de janeiro de 2023 e aceito em 28 de fevereiro de 2023

RESUMEN
El siguiente trabajo problematiza el cambio de paradigma en lo referente a la soberanía política con la influencia de la Inteligencia Artificial, lo que se da en llamar la nueva gobernanza digital. Expresiones como algocracia y vigilancia algorítmica han puesto de manifiesto un escepticismo cada vez mayor sobre el auge de nuevos modelos de gobernanza basados en el análisis de Big Data y la Inteligencia Artificial (IA). Surge, pues, la necesidad de repensar de qué manera el derecho hará frente a estos nuevos dilemas que están produciendo un cambio en la vida social e individual, teniendo en cuenta esta nueva vigilancia, definiendo en particular los espacios de permisión, so pena de movilizar nuevos criterios de resistencia.

Palabras claves: gobernanza. Inteligencia artificial. Big data. Derecho comparado**.**

ABSTRACT

The following paper problematizes the paradigm shift regarding political sovereignty with the influence of Artificial Intelligence, what is referred to as the new digital governance. Expressions such as algocracy and algorithmic surveillance have revealed a growing skepticism about the rise of new governance models based on Big Data analysis and Artificial Intelligence (AI). There is therefore a need to rethink how the law will deal with these new dilemmas that are bringing about a change in social and individual life, taking into account this new surveillance, in particular by defining the spaces of permission, on pain of mobilizing new criteria for resistance.

Keywords: governance. Artificial intelligence. Big data. Comparative law.

RESUMO

O seguinte problema no papel é a mudança de paradigma na soberania política com a influência da Inteligência Artificial, a chamada nova governação digital. Expressões como a algocracia e a vigilância algorítmica revelaram um crescente cepticismo sobre o surgimento de novos modelos de governação baseados na análise de Grandes Dados e Inteligência Artificial (IA). Há portanto necessidade de repensar a forma como a lei irá lidar com estes novos dilemas que estão a provocar uma mudança na vida social e individual, tendo em conta esta nova vigilância, em particular através da definição dos espaços de permissibilidade, sob pena de mobilizar novos critérios de resistência.

Palavras-chave: governação. Inteligência artificial. Grandes dados. Direito comparado.

1. INTRODUCCIÓN

En el contexto fluido de la modernidad líquida señalada por Bauman (2003), el poder se mueve a la velocidad de las señales electrónicas, mientras la transparencia aumenta para unos y disminuye para otros. La discusión en torno al concepto de soberanía, a lo largo de la historia del derecho político, ha sido un tema recurrente; con su desarrollo exponencial a partir de Jean Bodin (1530-1596)[1] en adelante, se buscó compatibilizar el poder con la juridicidad del Estado, lo cual sigue siendo uno de los principales problemas en nuestros días y la cuestión clave del Estado constitucional. Esto porque el nacimiento del Estado se identifica con el nacimiento y afirmación del concepto de soberanía. En la introducción al clásico libro *Elements de Droit constitutionnel francais et comparé,* Esmein (1921, 1) considera que Estado es la personificación jurídica de Nación, siendo que el constitutivo de esta se halla en la existencia de una autoridad superior a las voluntades individuales[2].

En este sentido, lo característico del paso de la Edad Media a la Moderna, consistió en la aceptación universal de la capacidad y superioridad legislativa del soberano político, la fuente principal del derecho sería en adelante la ley escrita emanada del poder humano y no la voluntad soberana o la costumbre, de manera que la legislación es un proceso mediante el cual lo jurídico fundamenta lo político. Ese mismo proceso seguirá mutando en la edad contemporánea, ya que como otrora fuera la ley el instrumento y la marca del poder político, ahora lo es el control de la información por medio de los mecanismos de digitalización y de inteligencia artificial.

En relación a los procesos de integración y globalización, la soberanía moderna enfrenta una crisis que la doctrina no ha dejado de analizar desde diversos campos. Entre ellos, los elementos que interesaban a la soberanía como lo eran principalmente la custodia del territorio y el orden de la población asentada en él, han mutado notoriamente. La centralización de los datos y la creación de amplias bases de los mismos, en forma automatizada fueron posibles ya que a lo largo de los siglos, los Estados adoptaron formas y procedimientos para recopilar información de los ciudadanos en función de diversas finalidades relacionadas con la soberanía y su ejercicio, así como la organización de una administración pública eficiente.

En este sentido, es que se comienza a mencionar en los debates contemporáneos la "soberanía de los datos", este término se utiliza en diversos sentidos, uno de ellos designa el derecho de los Estados en relación con otros para regular la recogida y la propiedad de los datos,

[1] En su clásica obra, *Les six livres de la république*, (París, reed. Fayard, 1986). I, 8, 179 el autor señala que la soberanía es el poder absoluto y perpetuo de una República".

[2] Allí define el Estado como "la autoridad superior" o "Soberanía" con que se halla investido, negando la posibilidad de otra potestad superior o concurrente.

incluido el acceso y la utilización de los mismos que se encuentran bajo su jurisdicción nacional[3]. La soberanía de los datos es el derecho de una nación a recopilar y gestionar sus propios datos (Rainie et al., 2017: 5-6). En particular, las normas que rigen cómo y dónde deben almacenarse determinados conjuntos de datos dentro de las fronteras nacionales y los derechos de los gobiernos a acceder a esos datos siempre que lo necesiten. Asimismo, la soberanía de los datos denota la inviolabilidad o integridad de los mismos. Es, por tanto, una incidencia del derecho soberano de los Estados en la medida en que se extiende y aplica a la gobernanza de la información recoplilada por la IA. Todo esto lo hacen sujetos de obligaciones contractuales y de los principios de colaboración que son fundamentales para el orden público en el ciberespacio.

2. EL ROL DE LA IA EN LA GOBERNANZA DIGITAL

La repercusión contemporánea que tiene la gobernanza digital (Jarke, 2019) nos motiva a indagar de qué manera estos nuevos avances tecnológicos impactan en los gobiernos estatales y en el ámbito de los derechos humanos. Es un hecho que el debate político se realiza cada vez más a menudo por medios electrónicos: los políticos y los ciudadanos discuten a través de las redes sociales; una muestra del poder de las mismas por ejemplo en el marketing político es el éxito que tuvo la primera campaña de Obama en EEUU, o la repercusión de los seguidores que a través de *twitter* logró Trump al asumir su presidencia. La información política está ampliamente disponible pero por otro lado, también es constatable que la mayoría de los procedimientos institucionales vinculados a los tres poderes: legislativo, ejecutivo y judicial, están todavía ligados a los mecanismos de acción del pasado, lo cual resulta de que tenemos algunos beneficios potenciales de la tecnología pero que no se aprovechan. Con todo es innegable que la inteligencia artificial desempeña un papel muy importante en la política de los Estados modernos.

La soberanía como concepto heredado de Europa tiene un significado primario vinculado con la autoridad suprema dentro de un territorio que se atribuye a un Estado. La territorialidad es un elemento fundamental de la soberanía, que sólo tiene autoridad dentro de un espacio geográfico definido con precisión. Esta característica de la soberanía explica por qué los macrodatos procesados por mecanismos de inteligencia artificial, son un obstáculo para los Estados. Esto porque pertenece a un ciberespacio que no es físico y, por tanto, no puede limitarse a un territorio, aunque su recopilación, almacenamiento, intercambio y transmisión se base en

[3] Cfr. El trabajo de Oguamanam, Chidi, ABS: Big Data, Data Sovereignty and Digitization: A New Indigenous Research Landscape (December 1, 2018).

componentes físicos como el *hardware*. De esta manera la intangibilidad de los macrodatos pone en tela de juicio el Derecho internacional tradicional en materia de jurisdicción.

En el contexto de las aplicaciones digitales de rastreo de contactos, la soberanía se entiende mejor como "una compleja red de tres actores -naciones, empresas (de grandes tecnologías) e individuos- que ejercen diversas formas de poder en contra o en nombre de los demás para reclamar y para debilitar o reforzar las reivindicaciones de soberanía de otros actores" (Tretter, 2023,1).

En concreto, la soberanía de los datos se inserta en la soberanía de los países: "a nivel nacional, la capacidad de acumular, procesar y utilizar grandes datos se convertirá en un nuevo hito del país" (Hummel, Patrik et al., 2021,7). De manera que "uno podría incluso afirman que la soberanía nacional está condicionada a una soberanía de datos adecuada. Si un país no dispone de controlar la información pública, será en parte disfuncional" (Irion, 2012, 53). La soberanía de los datos sería así como una extensión o un aspecto, de la soberanía absoluta: "la soberanía de los datos plantea un problema de política pública pertinente para los gobiernos de todo el mundo, porque es una dimensión crucial de la soberanía nacional que presupone el Estado nación" (Irion, 2012, 42).

Actualmente podemos constatar que la IA es objeto de análisis en múltiples disciplinas. En el caso que nos ocupa, dentro de las ciencias jurídicas no podemos soslayar la responsabilidad que conlleva la utilización y aprovechamiento de la misma. La Comisión Europea establece que:

> La IA es una tecnología estratégica que ofrece numerosas ventajas a los ciudadanos, las empresas y la sociedad en su conjunto, siempre y cuando sea antropocéntrica, ética y sostenible y respete los derechos y valores fundamentales. La Inteligencia Artificial aporta importantes mejoras de la eficiencia y la productividad que pueden reforzar la competitividad de la industria europea y mejorar el bienestar de los ciudadanos. También puede contribuir a encontrar soluciones a algunos de los problemas sociales más acuciantes, como la lucha contra el cambio climático y la degradación medioambiental, los retos relacionados con la sostenibilidad y los cambios demográficos, la protección de nuestras democracias y, cuando sea necesaria y proporcionada, la lucha contra la delincuencia (Comité Europeo, 2020, 67)[4].

Esto refiere a que es insoslayable pensar en los macrodatos y su asociación con una nueva noción de soberanía, a la cual podríamos llamar "soberanía digital"; esto implica la autonomía de un Estado en la regulación y protección de los datos de sus ciudadanos y la autodeterminación de los usuarios en el uso de sus datos personales. Los big data fluyen de un país a otro y se propagan en una constelación de redes digitales sin barreras estatales: se recogen en un país y pueden utilizarse en otros. Debido a esta dispersión, así como a la interdependencia global de los Estados,

[4] European strategy for data, de 19 de febrero de 2020. Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones.

los macrodatos desafían el concepto de soberanía estatal, que siempre implica un territorio físico circunscrito. Esta idea de soberanía digital nos conduce a apoyar una definida regulación jurídica del Internet a nivel nacional, así como la localización de datos, limitando el almacenamiento, movimiento y procesamiento de los mismos a zonas específicas.

Con esto queremos hacer hincapié en que como toda herramienta, la inteligencia artificial se puede utilizar con diversas connotaciones ético-jurídicas. Se percibe por las realidades que nos toca atravesar, que la "guerra" contemporánea ha devenido en una concentración por poseer los datos de los ciudadanos, como en algún momento la disputa fuera por el territorio o por el petróleo. Con lo pareciera tener el control militar quien tenga la hegemonía del ciberespacio, los gobiernos de todo el mundo están haciendo de la autonomía y soberanía digitales su estrategia económica, diplomática y de seguridad, (Barrios-Acedo, 2020). Esta disputa parece recaer entre dos grandes potencias: Estados Unidos y China, pues son los que poseen las redes y el monopolio de los datos. La "guerra comercial" digital (Ilves – Osula, 2020, 24) entre estas dos potencias sobre la tecnología de redes 5G y el software móvil que se ha desarrollado en el último año es el más reciente[5].

En estos tiempos biopolíticos sin precedentes posteriores a COVID-19, estas dinámicas pueden haber fomentado nuevos modos de ser un ciudadano digital en determinadas zonas urbanas, pues estos procesos de informatización llevaron a la aparición de regímenes de ciudadanía digital interrelacionados.

Al mismo tiempo que se contribuye a reformular la naturaleza del Estado-nación. Por un lado, en lo que respecta a la conciencia tecno-política de los datos, estas dinámicas implican abordar las preocupaciones sobre las tecnologías biométricas (por ejemplo, pasaportes con vacunas), y desplegar herramientas algorítmicas de identidad para la ciudadanía. Por otro lado, se relacionan con la creciente conciencia refundacional socioeconómica y la contrarreacción (por ejemplo, a través de la respuesta interna post-Brexit en Gales).

Expresiones como algocracia y vigilancia algorítmica han puesto de manifiesto un escepticismo cada vez mayor sobre el auge de nuevos modelos de gobernanza basados en el análisis de Big Data y la Inteligencia Artificial (IA). La IA es la inteligencia demostrada por las máquinas, en contraposición a la inteligencia natural mostrada de los seres humanos. En consecuencia, la IA permite a las máquinas acercarse cada vez más a las capacidades humanas para la percepción y el razonamiento en dominios estrechos (Calzada, 2022, 3). La creciente desconfianza entre las naciones ha provocado un aumento de la soberanía digital, que refiere a la

[5] Tres tecnologías principales (5G, la nube y la IA) ilustran las compensaciones detrás del dilema de la soberanía tecnológica y el reto que supone la creciente omnipresencia de las ofertas de software y servicios.

capacidad de una nación para controlar su destino digital y puede incluir el control sobre toda la cadena de suministro de la IA, desde los datos hasta el hardware y el software. La soberanía digital como posesión de infraestructuras nacionales independientes y seguras implica que un Estado puede inmiscuirse en la vida privada de los ciudadanos accediendo a sus datos personales a través de agentes de inteligencia y organismos encargados de hacer cumplir la ley y justificando la intrusión como una cuestión de seguridad. Una consecuencia de la tendencia hacia una mayor soberanía digital, es el creciente temor a quedar aislado de componentes digitales críticos como los chips informáticos y la falta de control sobre el flujo internacional de datos de los ciudadanos.

El segundo y más reciente concepto de soberanía digital se centra en la autonomía y autodeterminación de los usuarios en el ámbito digital. Esta autodeterminación se define como la capacidad de tomar decisiones sobre el uso de los propios datos personales, plataformas digitales y dispositivos de forma autónoma, competente e informada. Se han propuesto varias medidas para mejorar la soberanía de los usuarios sobre sus datos; por ejemplo, programas que proporcionen a los usuarios las competencias necesarias para actuar en el espacio digital (es decir, alfabetización digital) y les animen a reflexionar de forma crítica sobre las tecnologías digitales. Otras propuestas para mejorar la soberanía digital de los usuarios incluyen exigir a las empresas tecnológicas que cifren los datos de los usuarios y sean más transparentes sobre el uso que hacen de ellos.

Cabe destacar que muchas veces estos dos conceptos de soberanía digital entran potencialmente en conflicto; esta tensión es evidente en el caso de los macrodatos. Por un lado, cada Estado pretende ejercer su soberanía sobre el ámbito digital circunscripto en su territorio y, por tanto, proteger los big data de sus ciudadanos respecto de la vigilancia extranjera. Por otro lado, la soberanía digital de los ciudadanos sobre sus propios big data, así como la privacidad y seguridad de dichos datos, se ven amenazadas por la posibilidad de que el Estado pueda acceder a ellos.

3. DERECHO COMPARADO SOBRE EL PRESENTE DILEMA

El 29 de septiembre de 2021, el nuevo Consejo de Comercio y Tecnología (CCT) de Estados Unidos y la Unión Europea (UE) celebró su primera cumbre. Tuvo lugar en la antigua ciudad industrial de Pittsburgh, Pensilvania. Tras la reunión, Estados Unidos y la UE declararon su oposición a la inteligencia artificial (IA) que no respeta los derechos humanos y se refirieron a sistemas que vulneran los derechos. El objetivo implícito de la crítica era el sistema de "crédito social" de China, un sistema de big data que utiliza una amplia variedad de datos para evaluar la

puntuación de crédito social de una persona, que determina los permisos sociales en la sociedad, como la compra de un billete de avión o tren[6].

El Reglamento General de Protección de Datos (RGPD) de la Unión Europea, que entró en vigor en 2018, sentó un precedente para la regulación de los datos. Esta legislación a su vez ha inspirado otras leyes, por ejemplo, la Ley de Privacidad del Consumidor de California (CCPA) y la Ley de Protección de Información Personal de China (PIPL). El objetivo de estas nuevas leyes no es sólo garantizar el respeto de los derechos de los ciudadanos de la UE en el espacio digital, sino también asegurarse de que las empresas europeas tengan más posibilidades de competir con las grandes tecnológicas estadounidenses. El enfoque fundamental de la inteligencia artificial está basado en el respeto de los derechos humanos. Este enfoque se está poniendo lentamente en práctica para condenar el uso de la IA con fines de vigilancia y control social, como se observa en China, Rusia y otros países autoritarios.

Veamos en esta línea de análisis el caso del continente europeo, Podemos encontrar como punto de partida en esta presión por la soberanía tecnológica, las denuncias de espionaje a gran escala por parte de los servicios de Estados Unidos en el año 2013. Desde entonces, se han dado varios pasos que apuntan a la necesidad de una mayor autonomía, como la modificación de las normas de competencia de la Unión Europea para favorecer a los actores europeos, la creación de un sistema de pagos y los debates sobre nuevas normas de fiscalidad digital.

La Presidente de la Comisión Europea, Úrsula van der Leyen, se refirió específicamente en varias oportunidades a la "soberanía tecnológica" en su agenda inaugural:

> Del sector digital depende nuestro éxito o fracaso. Esto refleja la importancia de invertir en nuestra soberanía tecnológica europea. Tenemos que duplicar la inversión para moldear nuestra transformación digital de acuerdo con nuestras propias normas y valores. (…) El mismo carácter de las amenazas que afrontamos evoluciona rápidamente: de los ataques híbridos o los ciberataques a la escalada armamentística en el espacio. Las tecnologías disruptivas han venido a nivelar en gran medida el poder y su ejercicio por parte de los estados canallas o grupos no estatales, porque para causar estragos a gran escala ya no hacen falta ni divisiones armadas ni proyectiles. Basta un ordenador portátil para paralizar una fábrica, toda una administración municipal o un hospital. O con un simple teléfono inteligente conectado a internet se puede alterar el curso de unas elecciones[7].

[6] Cfr. Reportaje de Benjamin Cedric Larsen, December 8, 2022 en https://www.brookings.edu/research/the-geopolitics-of-ai-and-the-rise-of-digital-sovereignty/

[7] Ver en este sentido https://spain.representation.ec.europa.eu/noticias-eventos/noticias-0/discurso-sobre-el-estado-de-la-union-de-2021-pronunciado-por-la_es

El enfoque de la UE para regular la inteligencia artificial, señalado en el Reglamento recientemente propuesto por la Comisión Europea en abril de 2021, refleja una preocupación subyacente por la protección de los derechos y libertades de los ciudadanos de la UE. En este sentido, coincide con otras piezas clave de la legislación de la UE relacionadas con el uso de las tecnologías digitales, como el Reglamento general de protección de datos (Reglamento 2016/679). En todos los casos, los indudables beneficios potenciales prometidos por las nuevas tecnologías deben contraponerse a los riesgos que pueden plantear, ya sea por uso indebido o simplemente por inadvertencia (efectos no deseados), para los intereses individuales o sociales.

El proyecto de Reglamento sobre IA establece un marco que logrará un equilibrio adecuado entre los beneficios y los riesgos asociados a la tecnología. Este proyecto está actualmente en trámite legislativo en la UE, con la expectativa de que se promulgue como ley en 2023. Algunos usos de la IA cuyo riesgo se considera inaceptable dentro de este proyecto, están directamente prohibidos. Esto incluye los sistemas de IA que manipulan las opiniones o decisiones humanas mediante arquitecturas de elección, llevando a las personas -como individuos o grupos- a actuar en su detrimento, así como las tecnologías para la vigilancia indiscriminada.

En segundo lugar, otras aplicaciones, que contienen riesgos previsibles para la salud, la seguridad o los derechos fundamentales de las personas físicas, se clasifican como de "alto riesgo" (anexo II, COM 2021, 206 final). En este caso, su desarrollo estará sujeto a un riguroso proceso de evaluación de riesgos y acreditación para garantizar que los riesgos se minimizan y gestionan adecuadamente antes de que las aplicaciones salgan al mercado. Los desarrolladores tendrán que demostrar, entre otras cosas, la calidad, representatividad e idoneidad de los conjuntos de datos utilizados, la transparencia en el funcionamiento del sistema y su precisión, solidez y ciberseguridad (COM 2021, 206 final, Título III). En este sentido, ya existen varias soluciones de IA sanitaria con marcado CE -requisito normativo para comercializar un producto sanitario (Reglamento (UE) 2017/745)- en Europa.

En otros aspectos, sin embargo, el marco jurídico de la UE muestra una actitud abierta y de aceptación de las aplicaciones de la IA. Los sistemas de IA que queden fuera de las categorías prohibidas y de alto riesgo, es decir, de "bajo riesgo", pueden desarrollarse sin restricciones normativas. El único requisito residual en este caso es el de la transparencia (artículo 41)

Mientras tanto, la importancia de la protección de los derechos de los ciudadanos de la UE en relación con las aplicaciones de la IA se pone de relieve en la "Declaración Europea sobre los Derechos Digitales y la Década Digital" publicada por la Comisión en enero de 2022 (COM(2022) 28 final). En ella se afirma que: "Toda persona debe poder beneficiarse de las ventajas de la inteligencia artificial tomando sus propias decisiones con conocimiento de causa en

el entorno digital, al tiempo que se le protege contra los riesgos y daños para su salud, seguridad y derechos fundamentales" (Capítulo III). El dilema genera un debate sobre la "soberanía de los datos", ya que muchas empresas líderes del mercado a gran escala, por ejemplo, en la automoción, aerolíneas o construcción de maquinaria disputan la información. La privacidad de los datos tal y como se define, por ejemplo, en el Reglamento General de Protección de Datos europeo considera al ciudadano en un papel pasivo que debe ser protegido contra poderes a los que no puede enfrentarse en igualdad de condiciones.

Las restricciones a los actores digitales han adoptado una forma fragmentaria, cubriendo ciertas actividades específicas de alto riesgo, mientras que por lo demás dejan el campo libre para que las empresas innoven y prosperen. Otro factor es la fuerte protección de que goza la libertad de expresión en la Constitución estadounidense. Esto se refleja, entre otras cosas, en la actitud tolerante del legislador hacia la práctica -esencial para los modelos de negocio de muchas empresas de Internet- de la recopilación, el comercio y el análisis de datos a gran escala.

Por otro lado, se buscaría en vano una legislación general de protección de datos similar al GDPR, en EE.UU. pues allí se ha adoptado más bien un enfoque "de bolsillo" limitado a sectores concretos, como las normas de protección de datos sanitarios sensibles de la Ley de Portabilidad y Responsabilidad de los Seguros Sanitarios (HIPAA) de 1996. Más allá de estas áreas específicas de cobertura, se considera que se proporciona suficiente protección a los individuos a través del funcionamiento del mercado (donde los usos deshonestos de los datos se penalizan con la pérdida de la confianza y la buena voluntad del consumidor), así como la responsabilidad ex post facto en caso de daño individual probado, a través de agravios basados en la privacidad.

Esto muestra que a medida que las fronteras jurisdiccionales comienzan a difuminarse en el ciberespacio, los fundamentos territoriales convencionales de la soberanía ya no son tan sólidos como antes solían ser. Así por ejemplo, en el contexto de las investigaciones penales, los proveedores de servicios como Google y Facebook están ahora obligados (en virtud de la ley estadounidense CLOUD como en el marco propuesto por la UE para las pruebas electrónicas)[8] a compartir datos específicos con las fuerzas de seguridad nacionales e internacionales, independientemente de la de la ubicación física real de los datos.

El concepto de soberanía de datos ha dado lugar a la idea de "ecosistemas de datos impulsados por alianzas" con plataformas habilitadoras. Desde 2015, una alianza mundial de empresas y organizaciones de investigación llamada *International Data Space*[9] y una serie de proyectos de investigación estrechamente relacionados que han elaborado una arquitectura de

[8] Cfr. https://www.aecoc.es/innovation-hub-noticias/la-ley-cloud-gdpr-y-la-soberania-de-los-datos/
[9] https://internationaldataspaces.org/

referencia estandarizada para dichas plataformas habilitadoras, y la han probado en una amplia gama de casos en entornos industriales y sociales.

Uno de los ejemplos de instrumentalización política de la inteligencia artificial está dado por el uso de drones, los cuales son, esencialmente, robots voladores. En la actualidad, Estados Unidos lidera este campo, pero la tecnología se está difundiendo ampliamente y es cada vez más asequible. También se utilizan armas autónomas que combinan la tecnología de los drones con la inteligencia artificial y tienen el potencial de seleccionar y atacar objetivos sin intervención humana, según criterios previamente definidos. Una nueva generación de armas planeadoras hipersónicas está también a punto de entrar en este dominio, "aumentando la probabilidad de que el espacio desempeñe un papel importante en futuros conflictos, lo cual suscita la preocupación de que los actuales mecanismos para regular las actividades espaciales ya no sean suficientes" (Schwab, 2016, 70).

Por otro lado, haciendo alusión a dos grandes potencias como China y Rusia, podemos observar que en el caso de Rusia respecto a lo que hace al plano de la gobernanza de Internet, ilustra el intento de reafirmar su soberanía sobre el ciberespacio (tras un periodo inicial de no intervención en el mismo). En consonancia con China, Rusia tiende ahora a apoyar un modelo de gobernanza mundial de Internet centrado en el Estado, que favorece los acuerdos multilaterales en lugar de la configuración de múltiples partes interesadas (Nocetti, 2015, 115). Los enfoques destinados a reforzar la soberanía tecnológica y digital de Rusia han dado paso, desde principios de la década de 2010, a una serie de leyes e iniciativas. Desde 2014, el Gobierno ruso ha invertido considerables recursos en rediseñar su infraestructura de Internet (denominada "RuNet"), tanto para limitar el acceso a direcciones web específicas como para bloquear plataformas de mensajería (como Telegram), y también con el objetivo de controlar más directamente el tráfico de Internet a través del territorio ruso. Esta tendencia se ha acelerado aún más a raíz de la guerra en Ucrania.

4. HACIA DONDE SE DIRIGE EL DERECHO

Las normas son un instrumento político esencial en el ámbito de la IA y, más ampliamente, de la gobernanza digital, y tienen por objeto proporcionar una serie de beneficios para garantizar la calidad y seguridad esperadas, informar y favorecer la interoperabilidad y el comercio, etc. La literatura sobre gobernanza digital ha demostrado hasta qué punto las normas y los protocolos son notoriamente políticos (DeNardis, 2009), más aún a medida que las tecnologías digitales se generalizan en todo el mundo y en toda la sociedad. Algunos de ellos son "puntos de control" y pueden servir como forma de política pública (formulada sobre todo por organizaciones privadas

por ejemplo determinando cómo puede proceder la política de innovación y la competencia económica tanto a nivel nacional como mundial, o constituyendo cuestiones políticas sustantivas. Está claro, por tanto, que, desde un punto de vista más general, quien controle el sistema ideado por la gobernanza digital tendría un enorme poder. Por medio de las entidades supranacionales se crearía una especie de "gran hermano" capaz de controlar todos los datos que circulan por la web, incluyendo por tanto los correos electrónicos, los faxes, etc. (Fioriglio, 2005, 99).

Byung-Chul (2020) afirma que el dataísmo está estrechamente relacionado con los mecanismos de vigilancia como forma de controlar a las personas. La vigilancia, es uno de los motivos más básicos de la humanidad, en función del deseo de un segmento social de gobernar a otros segmentos. Como los motivos y deseos humanos dirigen el desarrollo de la tecnología, ésta también puede llevar estos motivos y deseos de las personas más allá de su competencia física. A lo largo de estos años, varias preguntas han surgido en relación con la revolución informática y la progresiva *datafication* de nuestra sociedad. En una sociedad cada vez más basada en la explotación de los datos, frente al riesgo de una distribución asimétrica del poder relacionado con la información y las posibles consecuencias en términos de discriminación y control social, se requiere una respuesta legal regulatoria no solo en cuanto a la protección de los datos sino también en lo referente al debate ético y social planteado por los usos de los algoritmos. En este sentido, las soluciones de vigilancia predictiva, por ejemplo, no son solo una cuestión de protección de datos o cumplimiento de la ley, sino que se refieren a las formas de sociedad y relaciones entre los ciudadanos y la administración que queremos adoptar en el futuro. Por lo tanto, las decisiones políticas sobre tecnologías similares instan a tener en cuenta también esta dimensión más amplia.

Además, la soberanía y el poder administrativo establecido por la ley prevén organismos públicos con facultades de legitimar la recopilación de datos de las personas sin ninguna posibilidad de negociación con los ciudadanos, salvo en los casos de gobiernos democráticos que la hicieron posible, si la información estaba relacionada con la naturaleza de las finalidades del tratamiento de datos. El procesamiento de datos ya no se centra en usuarios únicos (creación de perfiles individuales), sino que aumenta por escala y trata de investigar las actitudes y comportamientos de grandes grupos y comunidades. Las nuevas tecnologías y el poderoso *software* de análisis permiten recopilar y analizar grandes cantidades de datos para tratar de identificar patrones en el comportamiento de grupos de individuos y tomar decisiones que afectan las dinámicas internas de estos grupos, con consecuencias que influyen en los intereses colectivos de las personas involucradas.

Nos enfrentamos a preguntas igualmente complejas y de límite en el caso de la inteligencia artificial. Consideremos la posibilidad de máquinas que vayan un paso por delante de nosotros a la hora de razonar e incluso que piensen mejor que nosotros. Amazon y Netflix ya poseen algoritmos que predicen las películas y los libros que podríamos desear leer y ver. Los sitios de citas y búsqueda de empleo sugieren las parejas y los puestos de trabajo —en nuestro barrio o en cualquier parte del mundo— que sus sistemas creen que mejor se ajustan a nosotros. Cuando consideramos estos ejemplos y sus implicaciones para los seres humanos, nos adentramos en territorio desconocido, es decir, en los albores de una transformación humana diferente de cualquier cosa que hayamos experimentado.

La regulación del tratamiento de datos está evolucionando hacia una noción más amplia, enfocada por una dimensión colectiva del uso de los mismos. Esto impulsa al legislador a abordar los desafíos del nuevo paradigma que comporta el Big Data de una manera que abarca cuestiones relativas a la gobernanza de la sociedad y al papel de los ciudadanos. También se tiene en cuenta la necesidad de profundizar sobre la interacción entre los diferentes derechos fundamentales (Mantelero, 2018, 160).

Afirma Nye (2010) que los gobiernos más capaces y comprometidos están dispuestos a explotar su "ciberpoder", como una nueva forma de proyección de la soberanía, a veces empleando empresas bajo su jurisdicción y control como sus agentes. Aunque sus intenciones pueden ser benignas y sus acciones parecer incluso necesarias en un mundo globalizado -por ejemplo, la persecución de terroristas o el blanqueo de dinero, estas actividades hacen que la mayoría de los países sufra una "brecha de soberanía" y se encuentren preocupados por el estado de derecho interno. Se trata de una brecha que las nuevas políticas y la autonomía tecnológica pretenden llenar.

Cuando las naciones ejercen la soberanía biopolítica, perjudican la soberanía de sus ciudadanos, es decir, limitan su capacidad de tomar sus propias decisiones libres de coacción o manipulación. Sin embargo, no sólo las naciones, sino también las grandes empresas tecnológicas ejercen la soberanía y, por tanto, amenazan la autonomía de los individuos, y las aplicaciones de rastreo de contactos desempeñan un papel crucial en este sentido. Las empresas con grandes tecnologías, especialmente las plataformas digitales, vigilan a sus usuarios las veinticuatro horas del día y recopilan sus datos hasta el punto que saben, "más sobre nosotros de lo que nosotros sabemos de nosotros mismos" (Gray, 2019). Al recopilar los datos de sus usuarios, las empresas pueden comprometer la autonomía de los mismos, estableciéndose como "un nuevo tipo de soberano poder" (Zubof, 2015, p. 86).

Las consideraciones sobre las demandas de protección relacionadas con la soberanía de los datos son necesarias para decisiones ejecutables sobre los mismos (Hummel, Braun, & Dabrock, 2021). Así pues, en consonancia debería existir la posibilidad de que los seres humanos determinen las entidades que acceden a sus datos (Couture & Toupin, 2019), la finalidad para la que se procesan los datos, y la capacidad de valorar (u observar retrospectivamente) las consecuencias derivadas para la privacidad de las personas.

Otra situación que el derecho debería tener presente es la relación del uso de datos y de la tecnología en los conflictos bélicos. La soberanía de los Estados nación se reafirma digitalmente cuando utilizan su prerrogativa para cortar el acceso a Internet a poblaciones enteras. La guerra en Siria es un ejemplo para poner de relieve un giro desde el dominio del territorio al dominio en el Internet: los Estados nación tienen el poder de controlar si Internet fluye o no. Además, si se utiliza en el contexto de la guerra puede colaborar para reforzar la soberanía, y así vemos que esta tecnología se utiliza como un medio acrecentar el poder pasando de ser un objeto de comunicación o de información a una herramienta que puede cambiar el destino de los pueblos y los derechos humanos de los ciudadanos que cada vez se encuentran más amenazados por las grandes empresas de big data.

5. CONCLUSIÓN

En estas páginas hemos esbozado el cambio significativo respecto al enfoque "territorial" que prevalecía hasta ahora en materia de soberanía, la localización de los datos pasa a ser el principal factor de conexión determinante para identificar el Estado extranjero con el que iniciar un proceso de Asistencia Legal Mutua, a fin de obtener el acceso a las pruebas digitales, aunque la cuestión no termina ahí. El efectivo nexo para controlar grandes franjas del funcionamiento de una sociedad -transporte, vivienda, energía, salud alimentación, servicios financieros- se está desvinculando de la jurisdicción territorial donde se presta el servicio, con el proveedor de servicios sujeto a órdenes de su país de origen o de un tercer país.

Un punto de fuga sobre el cual se podría también analizar estos cambios tiene que ver con el mundo del Blockchain, tan en boga en los últimos años. El Blockchain, con sus características distintivas puede desafiar la soberanía estatal. Es notable la capacidad que posee de distribuir el control y la autoridad sobre los datos. Con el potencial de facilitar las transacciones sin intermediarios y hacer que algunas instituciones legales sean redundantes, conlleva grandes promesas y riesgos para las instituciones públicas. Todo el mundo de las criptomonedas, amenazan los monopolios clásicos de los Estados en ámbitos como la política monetaria, fiscal y social.

Si en la antigüedad la lejanía espacial era un antídoto contra la vigilancia y el control, esto ya no es posible, puesto que en la sociedad de la información el espacio pierde su significado tradicional y la vigilancia electrónica adquiere un papel central. Así reflexiona Ágata-Mangiameli, (2019, 107-124) respecto a que sería un error considerar la vigilancia electrónica como una simple y enésima reproposición de la moderna relación supervisor-supervisado, ya que el control es ahora continuo, automático e involuntario.

Mientras que las fronteras territoriales determinan los límites de los poderes de investigación y vigilancia de la policía en virtud del Derecho penal, varios ejemplos recientes demuestran cómo las nuevas formas de vigilancia extraterritorial que permiten a la policía acceder a las comunicaciones en línea de ciudadanos extranjeros y a la información digital almacenada en paraísos fiscales, cambia este paradigma enmarcado en el territorio dando paso a la soberanía digital.

Los casos de enjuiciamiento por represalias ante denuncias de delitos de Estado o espionaje en línea por parte de denunciantes plantean varios retos adicionales para los principios establecidos de soberanía territorial. Esta paradoja ya se encuentra instalada y las prácticas de comunicación desplazan el papel del territorio como principal método para limitar la vigilancia de las fuerzas del orden en virtud del derecho penal.

Pero esta vigilancia es cada vez más sofisticada y el tratamiento informático de datos se está convirtiendo en la norma, independientemente de las limitaciones que algunos legisladores intentan imponer a estas actividades. Por ejemplo, no es fácil garantizar que los datos personales se conserven sólo durante el tiempo prescrito por la legislación aplicable a cada caso concreto. Esto crea una memoria digital que, aunque fragmentada en una multiplicidad de bases de datos, representa una versión aún más terrible de un hipotético panóptico digital: todo lo que hacemos puede ser almacenado, nuestros actos y palabras pueden ser sometidos a innumerables juicios tanto hoy como en un futuro indefinido e indefinible (Fioriglio, 2014).

Por ejemplo, las leyes estadounidenses validan la vigilancia masiva de ciudadanos no estadounidenses que utilizan servicios en línea operados por empresas de este país. La clasificación legal de los datos electrónicos como propiedad controlada por corporaciones como Twitter o Microsoft pasa por alto la concepción del estatus personal que caracteriza al usuario final de esos datos.

Estos planteos que hemos querido esbozar es a fin de que reflexionemos acerca del profundo cambio que la política está sufriendo y el modo en que esta revolución tecnológica repercute en la crisis de las instituciones. La democracia se basa en la esfera pública, los ciudadanos tienen que tener poder de decisión aunque de forma indirecta en las cuestiones que

hacen al orden político, pero resulta que los dispositivos de inteligencia artificial influyen notoriamente en la formación de opinión de la ciudadanía.

En la sociedad contemporánea, el binomio "intimidad y seguridad" parece dar paso a "vigilancia y seguridad": así, la problemática conquista del reconocimiento, por parte de muchos Estados, del derecho a la intimidad como fundamental se ve cuestionada por las constantes e innumerables alarmas de seguridad. El poder predictivo de la inteligencia artificial y el aprendizaje automático hace que nuestro comportamiento en cualquier situación se vuelva predecible, ¿cuánta libertad personal tendríamos o sentiríamos al diferir de la predicción?; ¿podría este desarrollo llevar tal vez a una situación en la cual los mismos seres humanos comiencen a actuar como robots? Esto también conduce a una cuestión más filosófica, vinculada a cómo mantenemos nuestra individualidad en la era digital.

Los datos masivos se han convertido en la nueva materia prima –el nuevo petróleo– codiciado por los operadores económicos, siendo una fuente inmaterial inagotable de generación de riqueza (Morente Parra, 2019, 231). La perspectiva de los “daños múltiples” que pueden generar las nuevas tecnologías en general y Big Data en particular, nos lleva a adoptar una mirada crítica desde los derechos fundamentales. El artículo 22.1 del Reglamento General de Protección de Datos, trae la novedad de introducir la necesidad de proteger a los individuos ante la posibilidad de que puedan ser objeto de decisiones basadas únicamente en el tratamiento automatizado de datos y que éstas puedan tener efectos jurídicos o similares.

El “ciudadano digital” se estaría dejando transformar en “súbdito digital”, perdiendo así el dominio sobre su propia información personal y, por consiguiente, su identidad. Quizá en el contexto digital sea ilusorio entender que el desarrollo de nuestra personalidad es verdaderamente libre y autónomo, y haya llegado el momento de asumir que la construcción de nuestra identidad personal no depende únicamente de nuestras libres decisiones, sino que también “encuentra una fuente heterónoma, distorsionadora de la percepción que tiene cada individuo de su propia identidad, como única e intransferible” (Morente Parra, 2021, 224).

Según la concepción clásica de la soberanía estatal, un Estado es soberano cuando goza de pleno control sobre su territorio, de autoridad exclusiva a nivel interno y de independencia de la autoridad exterior. Estos aspectos de control y autoridad se manifiestan además en la elaboración y aplicación de las leyes. Como los macrodatos son intangibles y se extienden en redes que cruzan las fronteras de los Estados, no pueden regularse fácilmente con métodos basados en la soberanía del Estado sobre un espacio físico finito y conocible. La naturaleza intangible de los macrodatos trasciende la normativa estatal. Por lo tanto, la recopilación, el almacenamiento, el intercambio y

la transmisión de macrodatos deben abordarse mediante la coordinación y la cooperación entre Estados.

De este modo, es claro que la inteligencia artificial converge para organizar el fin de lo político, entendiendo lo político como la expresión de la voluntad general de suspender las decisiones, dentro de la contradicción y la deliberación, para responder lo mejor posible al interés común. La soberanía de los datos sobre la cual hemos reflexionado en este trabajo se refiere a la autodeterminación de los individuos y las organizaciones en cuanto al uso de esa información, tiene como objetivo permitir los acuerdos de uso de datos claramente negociados. Así es que los métodos y herramientas de seguridad informática desempeñarán en un futuro cercano, un importante papel de apoyo socio-técnico para hacerlo posible.

6. REFERENCIAS BIBLIOGRÁFICAS

Agata, Cecilia – Mangiameli, Amato, "Algorithms and Big Data. The Rules and Principles of Robotics", *Rivista di filosofia del diritto N° 1*, 2019, pp. 107-124.

Barrios, Miguel Ángel – Acedo, Enrique, *Geopolítica, soberanía y orden internacional en la nueva normalidad*, Buenos Aires, Biblos, 2020.

Bauman, Zygmunt, *Modernidad líquida.* México: Fondo de Cultura Económica. 2003.

Bodin, Jean, *Les six livres de la république*, París, reed. Fayard, 1986.

Byung-Chul, Ha, *Psicopolítica. Neoliberalismo y nuevas técnicas de poder*. Barcelona, Herder, 2020.

Calzada, Igor, *Emerging digital citizenship regimes: Pandemic, algorithmic, liquid, metropolitan, and stateless citizenships*, Citizenship Studies, *25(6-8). Special Issue 'Digital Citizenship in the Post-Pandemic Urban Realm'* .2022, pp. 1-30.

Couture, S., & Toupin, S. (2019). What does the notion of "sovereignty" mean when referring to the digital? New Media & Society(21), Article 10, 2305–2322

DeNardis, Laura, *Protocol politics: The globalization of Internet governance*. Cambridge. Mit Press, 2009.

Esmein, Adhémar, *Elements de Droit constitutionnel français et comparé*, París, Librairie de la societé Recueil Sirey, 1921.

Fioriglio, Gianluigi, "La nuova frontiera del controlloglobale: iltrustedcomputing, frainvoluzioneinformatica e criticitàgiuridiche", *Nomos* 3, 2005, pp. 87-102.

Fioriglio, Gianluigi, "Sorveglianza e controllo nella società dell'informazione. Il possibile contributo dell'etica hacker", *Nomos 2,* 2014, pp. 1-20.

Gray, J. (2019). The new tech totalitarianism. When companies know more about us than we know about ourselves. The New Statesman. https://www.newstatesman. com/culture/2019/02/the-new-tech-totalitarianism

Hummel, P., Braun, M., Augsberg, S., Ulmenstein, U. V., & Dabrock, P. (2021). Datensouveränität: Governance-Ansätze für den Gesundheitsbereich (1st ed.). Springer Nature.

Hummel, Patrik et al., *Data sovereignty: A review. Big Data & Society*, *8* (1), 2021, pp.1-17.

Ilves, Luukas – Osula, Anna-Maria, "The Technological Sovereignty Dilemma – and How New Technology Can Offer a Way Out" *European Cyber security Journal* 6, N°1, 2020, pp. 24-26.

Irion Kristina, "Government cloud computing and national data sovereignty", *Policy & Internet* 4 (3–4), 2012, pp. 40–71.

Jarke, Matthias et al., "Data Sovereignty and Data Space Ecosystems", *Business and Information Systems Engineering,* Vol. 61, N° 5, 2019, pp.549–550.

Libro Blanco sobre inteligencia artificial, un enfoque europeo orientado a la excelencia y a la confianza. Comisión Europea, Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones, *Configurar el futuro digital de Europa*, Bruselas, 19.2.2020, COM (2020) 67 final.

Mantelero, Alessandro, **"C**iudadanía y gobernanza digital entre política, ética y derecho" en Tomás de la Quadra-Salcedo- José Luis Piñar Mañas, *Sociedad digital y derecho,* Madrid*,* Imprenta Nacional del Boletín Oficial del Estado, 2018, pp. 159-178.

Morente Parra, Vanesa, (2019). "Big data o el arte de analizar datos masivos. Una reflexión crítica desde los derechos fundamentales", en *Derechos y libertades* Número 41, Época II, pp. 225-260.

Morente Parra, Vanesa, (2021). "La libertad de los modernos en la sociedad digital: el control de los datos os hará libres", en *Derechos y libertades,* Número 45, Época II, pp. 199-231.

Nocetti, Julien, "Contest and conquest: Russia and global internet governance", *International Affairs,* 91(1), 2015, pp. 111-130.

Nye, Joseph, *Cyber power*, USA, Harvard, 2010.

Oguamanam, Chidi, *ABS: Big Data, Data Sovereignty and Digitization: A New Indigenous Research Landscape*. Oguamanam, Chidi, ed. Genetic Resources, Justice and Reconciliation: Canada and Global Access and Benefit Sharing, ed (Cambridge: Cambridge University Press, 2018), Ottawa Faculty of Law Working Paper No. 2019-14, Available at SSRN: https://ssrn.com/abstract=3326282

Pohle, Julia, "Digital sovereignty", Internet *Policy Review*, 9 (4), pp. 1-19.

Rainie, Stephanie Carroll et al., "Data as a Strategic Resource: Self-determination, Governance, and the Data Challenge for Indigenous Nations in the United States", *The International Indigenous Policy Journal,* 8(2). 2017.

Schwab, Klaus, *La cuarta revolución industrial,* Barcelona*,* Debate, 2016.

Tretter, Max, Sovereignty in the Digital and Contact Tracing Apps. *DISO* 2, 2 (2023).

Zubof, S. (2015). Big other: Surveillance capitalism and the prospects of an information civilization. Journal of Information Technology, 30(1), 75–89. https://doi.org/10.1057/jit.2015.5

Sobre a autora:

Yamila Eliana Juri
Doctora en Derecho (Uncuyo), Abogada (UM), Profesora Universitaria en Ciencias Jurídicas y Sociales (Uncuyo), Licenciada en Filosofía (UNSTA), Investigadora posdoctoral de CONICET. Actualmente es Profesora de Filosofía del Derecho en la Universidad de Mendoza, Derecho Constitucional (Universidad Maza), Derecho Político (Universidad Nacional de Cuyo). Entre sus trabajos vinculados con el presente trabajo se destacan el nacimiento de la doctrina sobre la soberanía política y sus vinculaciones con el derecho internacional, con una tesis titulada "La soberanía como fundamento de la república en Jean Bodin. Una perspectiva jurídica" (2019). Recientemente abordó algunas cuestiones sobre inteligencia artificial y la soberanía centrándose en el manejo de datos. También se ha interesado en otro orden el derecho a la verdad y el fenómeno de la denominada "posverdad" sobre todo en el cambo educativo.
Universidad Nacional de Cuyo-Conicet y UNIVERSIDAD JUAN A. MAZA., Mendonza, Argentina
ORCID: https://orcid.org/0000-0002-3136-4144
E-mail: yamilajuri@gmail.com