La vigilancia algorítmica y el rol del Estado en la era digital

Jesús Manuel Niebla Zatarain*
Juan Ramón García-Feregrino**

Resumen:

El presente artículo aborda la adopción de técnicas de vigilancia algorítmica como herramientas que permitan al Estado garantizar la seguridad de sus ciudadanos y el ejercicio de la ley, así como la posible colisión de esta tecnología con los derechos humanos. Esta investigación se realizará con base en una metodología cualitativa, documental y deductiva para obtener las variables necesarias para el estudio correspondiente. El objetivo del presente artículo es brindar, tanto a los operadores jurídicos como al sector académico, una base sólida que les permita comprender las implicaciones jurídicas que la adopción de tecnología de vigilancia supone en la relación ciudadano-sector público.

Abstract:

The current article presents the implication of adopting algorithmic surveillance as tools that allow the State to guarantee security and the rule of law, as well as the potential collision of this technology with legal status of its citizens. This research will be carried out through a qualitative, documentary and deductive methodology to obtain the necessary variables for the corresponding study. The objective of this article is to provide both legal operators and the academic sector with a solid foundation that allows them to understand the legal implications that the adoption of surveillance technology implies in the citizen-public sector relationship.

* Doctor en Derecho, Profesor-Investigador de la Facultad de Derecho de la Universidad Autónoma de Sinaloa.

** Licenciado en Derecho por la UAM-A., Miembro de la Red de Investigadores Parlamentarios en Línea (REDIPAL).

Introducción

La relación entre gobierno y tecnología parece ser, en el presente, un elemento necesario e indispensable para que los Estados puedan cumplir y satisfacer de manera positiva el papel que tienen frente a las sociedades. En este sentido, no resulta inusual la utilización de Tecnologías de la Información y Comunicación (TIC) como instrumentos de apoyo para la realización de actividades administrativas en del sector público. Esta relación ha impactado de manera positiva la percepción que la ciudadanía guarda con respecto a la función de diversas dependencias estatales, lo que ha generado un mayor cumplimiento de obligaciones por parte de la ciudadanía, así como el mejoramiento de la interacción entre estos sectores. No obstante, la evolución tecnológica supone la implementación de enfoques basados en nuevas tecnologías, las cuales modifican la relación tradicional entre la ciudadanía y el sector público.

En este sentido, destaca la denominada gubernamentalización algorítmica. Este enfoque hace referencia a la vigilancia y control social con tecnología digital e Internet, lo cual lo convierte en uno de los temas de mayor relevancia en diversas sociedades, ya que estos dispositivos están siendo aplicados para la organización de sistemas de control y sanción sin que existan límites y lineamientos de operación debidamente definidos.

Tal escenario representa un nuevo peligro para los estados contemporáneos y sus democracias, ya que se pudiera criminalizar injustificadamente a ciudadanos con la generación de consecuencias jurídicas derivadas de falsos-positivos. Esto representa un aspecto en suma preocupante para la adopción de esquemas inteligentes en la aplicación de justicia, ya que podrían convertirse en elementos de afectación directa a los derechos humanos de los ciudadanos.

Los temas anotados previamente, habrán de ser desarrollados en el presente artículo, señalando el aspecto técnico de esta tecnología para efectos de responsabilidad, así como una propuesta para permitir que su operación replique principios jurídicos aplicables.

I. Gobierno-digital y el nuevo entorno social

Una de las principales aportaciones de las TIC al ámbito social, es el denominado gobierno electrónico (E-Gobierno). Este enfoque abarca diversas tareas

de la administración pública, las cuales refieren desde el acceso y digitalización a los servicios públicos, hasta la adopción de tecnología inteligente para la implementación de políticas públicas.[1]

El Estado, al ser el principal encargado de promover estrategias de mejoramiento y desarrollo en favor de la sociedad, resulta particularmente solicitado desde cuatro sectores básicos: la salud, la educación, la seguridad, tanto interna como la defensa nacional, y la administración interna del Estado.[2] Como parte de la naturaleza organizacional de estas operaciones, resulta evidente el procesamiento de información de diversa índole que permita garantizar el cumplimiento de los objetivos trazados por el ente público.[3] De manera relevante, la utilización de datos personales resulta fundamental para conocer las características de un grupo social en particular, así como para conocer sus necesidades prioritarias y establecer estrategias que permitan su solución.

No obstante, como parte de esta creciente necesidad de concentración de datos de las sociedades e individuos, surgen dudas sobre la legitimidad de dichos procesos y el uso que el Estado hace de esta, particularmente en lo relativo a vigilancia. Este escenario adquiere cada vez mayor relevancia, ya que al ser una sociedad en franca transición hacia un modelo digital, existen diversos procesos cotidianos, los cuales requieren de la información personal de los ciudadanos para brindar un servicio determinado aun y siendo este desempeñado por un ente particular.[4]

Esto ha traído como resultado una nueva interacción del sector privado y el público derivado de la capacidad del primero para captar de manera masiva datos personales, lo que los convierte *de facto* en elementos clave para el éxito de diversas estrategias públicas, particularmente de seguridad.

Un caso relevante es la operación llamada *Whitetamale*, llevada a cabo por la *National Security Agency (NSA)* de los Estados Unidos de Norteamérica, en donde se tuvo acceso a información confidencial de los mandatarios mexicanos Felipe Calderón Hinojosa y Enrique Peña Nieto, así como de varios

1 Alessandro Mantelero, "Ciudadanía y Gobernanza Digital entre Política, Ética y Derecho", p. 178.

2 María Belén Abdalá, *et al*., "La política de la inteligencia artificial: sus usos en el sector público y sus implicancias regulatorias", p.10.

3 Chris Berg, *The Classical Liberal Case for Privacy in a World of Surveillance and Technological Change*, p. 131.

4 Ver: Atenea Romina González Vega, "La Era de Vigilancia de Obama", p. 83.

funcionarios pertenecientes a la Secretaría de Seguridad Pública de México, que operan en el combate contra el narcotráfico y el tráfico de personas.[5]

La vigilancia algorítmica demuestra ser un avance para los gobiernos en el establecimiento y el registro basados en las TIC, el cual se ve complementado con datos biométricos, por lo que eleva su capacidad de identificación. Sin embargo, permiten ilustrar la capacidad de vigilancia e identificación de los ciudadanos en un entorno particular.[6] Esto termina por generar cuestionamientos éticos relativos a la factibilidad de utilizar esta tecnología en escenarios de prevención y vigilancia social masivos. De manera particular, sobresale su potencial implementación como dispositivos de seguimiento para aquellos grupos sociales o individuos no afines al Estado. Este escenario se abordará de manera detenida en el siguiente apartado.

II. La adopción de modelos de vigilancia digital: un riesgo tentativo

La transición hacia plataformas digitales ha dado lugar a la adopción de algoritmos en diversos campos, que van desde simples herramientas generales de investigación, hasta sistemas avanzados de vigilancia, junto con el registro de datos y la elaboración de perfiles, administran diversas organizaciones, entre otros.[7]

De manera particular, existen varias tendencias e iniciativas gubernamentales cuyo objetivo es mejorar la capacidad de vigilancia y detección de posibles delincuentes o terroristas, también alimentan la creciente aprensión de que el futuro presenta una versión acaso reducida de la privacidad.[8]

En este contexto, la vigilancia algorítmica realiza operaciones relativas a la detección automática de comportamientos anómalos y amenazas en espacios concurridos, lo cual ha sido un proyecto destinado a facilitar la protección de los ciudadanos. De esta manera, desarrolla una serie de perfiles con caracte-

5 David Price, *The New Surveillance Normal: NSA and Corporate Surveillance in the Age of Global Capitalism*, p. 48.

6 Atenea González Vega, *op. cit*., p. 86.

7 *Ibidem* p. 91.

8 *Ibidem*, p. 100.

rísticas determinadas que permiten a las autoridades operar bajo esquemas preventivos, lo cual significa la disminución de la afectación de ciertas conductas. Consecuentemente, los objetivos principales inherentes al debido establecimiento de esta tecnología, señalan.[9] (i) la confidencialidad de los datos y (ii) la integridad de los datos, y hacer que los datos (iii) estén disponibles (es decir, la disponibilidad) para los usuarios autorizados.

En la actualidad, el Estado se encuentra en una disyuntiva en materia de seguridad, derivado del hecho de que la mayoría de las amenazas se gestan y, en ocasiones, ejecutan desde entornos digitales. Esto influye en el reforzamiento de estrategias de seguridad digital, las cuales están basadas en el reconocimiento de patrones y la proyección de un potencial crimen.[10]

Esta realidad termina por afectar, de manera irremediable, la procuración de justicia, adecuándola a las particularidades del entorno digital e incrementando la adopción de medios de vigilancia compatibles con ese entorno. No obstante, aquí surge la discusión sobre el costo aparejado de esta tecnología, el procesamiento masivo de datos personales y la consecuente invasión a la privacidad de los ciudadanos, son los principales cuestionamientos. Estas particularidades habrán de solucionarse conforme la interacción entre el derecho y esta rama tecnológica se fortalezca, identificando elementos positivos y aplicando principios operativos en beneficio de la esfera jurídica de los ciudadanos.

III. Vigilancia algorítmica e inteligencia artificial

Uno de los principales esquemas preventivos en materia de entornos digitales, es la vigilancia algorítmica. Este proceso está basado en técnicas de minería de datos, las cuales procesan y filtran grandes volúmenes de datos, para después ser separados utilizando criterios determinados.[11] El proceso de perfilamiento llevado a cabo por estos dispositivos, replica diversas técnicas de inteligencia artificial, particularmente el denominado aprendizaje pro-

9 Pati Prasanthi, *et al*., *Privacy and Challenges to Data-Intensive Techniques*, p. 162.

10 Fernando Miró Linares, *Inteligencia artificial y justicia penal: más allá de los resultados lesivos causados por robots*, p. 98.

11 Tarleton Gillespie, *Algorithm*, pp. 18-30.

fundo,[12] el cual desarrolló representaciones, situaciones según la presencia y combinación de determinados datos en un contexto específico. A diferencia de otras vertientes predictivas, propias del aprendizaje automático, el aprendizaje profundo combina la capacidad de procesamiento de información con la generación de resultados a través de procesos de razonamiento humano. De esta forma, la vigilancia algorítmica emula a un operador humano realizando tareas de análisis y predicción situacional, pero en una escala mucho mayor.

Eso termina por replantear la relación entre el Estado y los gobernados, el cual deja de ser un un fenómeno estático para convertirse en una cadena de eventos altamente dinámicos e interdependientes, los cuales cuentan con la particularidad de surgir en entornos digitales y producir efectos jurídicos en escenarios físicos. Consecuentemente, al abordar este fenómeno desde la perspectiva del derecho a la privacidad y a los datos personales, se presenta un nuevo escenario donde las posturas tradicionales de aplicación de la ley tienen poco o ningún efecto como elementos reguladores.

En este sentido, si bien es cierto que el objetivo original de la vigilancia algorítmica es la identificación de potenciales perpetradores o participantes en la comisión de una actividad delictiva particular, su operación no siempre resulta compatible con el marco jurídico. Este enfoque es particularmente perjudicial para los derechos humanos y es aquí donde radica el reto principal en la masificación de esta perspectiva tecnológica: el garantizar que la ejecución de dicho enfoque operativo no vulnere sectores tradicionalmente perjudicados como minorías, disidentes y grupos políticos contrarios. Lo anterior, supone interpretaciones erróneas por parte de estos dispositivos, pueden perjudicar no sólo la privacidad y el debido procesamiento de datos personales, sino también la libertad de expresión e, incluso, el acceso a la información.

Consecuentemente, la vigilancia algorítmica resulta, entonces, un proceso de supervisión masiva, la cual depende del constante procesamiento de información personal obtenida por el tratamiento de datos por medio de dispositivos digitales. Si bien es cierto que se ha abogado por la utilización ética de esta tecnología, la realidad señala que opera desde un enfoque universal, diseñado bajo preceptos que no reflejan un interés inmediato de

[12] Maciej Mazurowski, *et al*., "Deep learning in radiology: An overview of the concepts and a survey of the state of the art with focus on MRI", p. 498.

seguridad, sino esquemas de control y seguimiento los cuales no incluyen como elemento ningún precepto de privacidad ni de debido procesamiento de datos personales.

IV. Tecnología, vigilancia y derechos humanos: hacia un nuevo convergente

La vigilancia algorítmica es uno de los adelantos tecnológicos de mayor impacto frente a los derechos humanos. Uno de los escenarios más importantes donde se expresa este fenómeno es en la administración pública, particularmente la administración de justicia. Paralelo a los modelos de gestión de información jurídica, este sector se encuentra experimentando con modelos predictivos que permitan impedir la comisión de delitos.[13]

Este enfoque de gobernanza multinivel, pone en el centro de la toma de decisiones la participación de los distintos actores para discutir los diferentes puntos de vista sobre la privacidad y la vigilancia que darán lugar a diferentes perspectivas de las partes interesadas sobre la recopilación, el procesamiento, la retención y la seguridad de los datos personales.[14]

Los Estados tienen la obligación de no interferir arbitrariamente con las libertades personales,[15] salvo algunas excepciones previamente establecidas, las cuales deben tener como premisa la defensa del bien y seguridad social, siendo encuadrables en estos supuestos los escenarios que los requieren.

En lo relativo a los datos personales, las excepciones presentadas por los organismos de seguridad se desprenden generalmente de investigaciones criminales, permitiendo a la autoridad decidir lo que necesitan y lo que deben hacer, involucrando al público por mandato, no por consentimiento.[16] Esta relación afecta de manera negativa la interacción sector público-ciudadano, generando desconfianza y trastocando la cooperación entre ambas partes, la cual, paradójicamente, debería de mejorarse por la inclusión de dicha tecnología.

13 María Belén Abdalá, *et al*., *op. cit*., p. 14.

14 Jack Caravelli y Nigel Jones, *Cyber Security: Threats and Responses for Government and Business*, p. 103.

15 Jose Antonio Carrillo Donaire, *La Compra Pública de Innovación en la Contratación del Sector Público*, p. 169.

16 Ana Delgado, *Technoscience and citizenship: Ethics and governance in the digital society*, p. 86.

A pesar de que este escenario ha sido abordado en diversas declaraciones, el uso inmoral de esta tecnología ha sido escasamente debatido y los esfuerzos regulatorios, ignorados, cuestionando la capacidad de protección de lineamientos como el Reglamento General de Protección de Datos (RGPD) de la Unión Europea.

El uso indiscriminado de la vigilancia masiva de datos viola tanto la privacidad como la autonomía de los titulares de estos, ya que afecta la individualidad de los ciudadanos, lo que afecta de manera negativa el funcionamiento de una democracia.[17] Esto termina por generar el replanteamiento del rol del individuo en entornos democráticos, donde la tecnología digital desempeña un papel fundamental para el desarrollo de diversas actividades sociales.

De igual forma, las consecuencias de esta tecnología en el ámbito privado de los ciudadanos, no se restringe a la confidencialidad de la información, repercute en la gestión y el uso adecuado de los datos personales.[18] En el contexto de la vida inteligente, los problemas de privacidad se extenderán a la vigilancia injustificada a través de diversas tecnologías, tanto domésticas como urbanas, por ejemplo, cámaras de seguridad o sensores de consolas de juego, y no simplemente a la gestión de datos personales.

Ante la inevitabilidad de este escenario, han existido diversos esfuerzos enfocados a minimizar el potencial efecto negativo de estas tecnologías. En este punto, los Tribunales de Derechos Humanos han buscado generar condiciones y requerimientos necesarios para que sean aplicables estas medidas, las cuales terminan por volverse inoperantes ante la evolución propia de la tecnología o bien, la simple opacidad de sus desarrolladores, lo cual termina por confirmar la necesidad de volver a comprender el rol de estas prerrogativas en entornos digitales.[19]

Desde una perspectiva procesal, la vigilancia algorítmica puede generar diversas controversias, toda vez que el mero perfilamiento puede resultar insuficiente para ligar a un individuo de manera indubitable con la realización de un ilícito.[20] Por otra parte, al abordarlo desde la perspectiva del principio de

17 Edison Lanza, "Los principios que garantizan una Internet libre, abierta y inclusiva de todas las personas y grupos sociales", p. 509.

18 Caravelli y Jones, *op. cit*.

19 Eleni Kosta, "Algorithmic state surveillance: Challenging the notion of agency in human rights", p. 6.

20 Jordi Nieva Fenoll, *Inteligencia artificial y proceso judicial*, p. 152.

presunción de inocencia, resulta de igual forma preocupante, ya que pudiera crearse una postura que influya en la preconcepción del individuo, afectando la actividad de operadores judiciales y fuerzas de seguridad. De igual forma, el derecho al acceso a la justicia resulta tergiversado, generando la percepción de estar restringido a determinadas clases sociales en perjuicio de otras.

Finalmente, la adopción de esta tecnología supone un reto para el sector jurídico, toda vez que resulta importante para mitigar la realización de conductas delictivas en entornos digitales. No obstante, el esquema de masificación de datos personales sobre el cual opera, supone sacrificar el ámbito de protección tradicional ofrecido por los derechos humanos.

V. Conclusiones

El advenimiento y diseminación de la tecnología digital requiere de la adopción de estrategias convergentes para la prevención y perfilamiento de conductas delictivas en dichos entornos. Esto ha traído como consecuencia la adopción de enfoques basados en la captación masiva de datos personales, lo cual representa un serio riesgo para los titulares de estos, particularmente en el caso de la vigilancia algorítmica. Para atender esto desde una perspectiva que, capaz de resguardar este y otros derechos humanos, se propone dotar a esta tecnología con la capacidad de adecuar su operación a lo establecido por el marco jurídico, combinando la eficiencia técnica con la jurídica. Esto resulta especialmente relevante en una etapa donde la sociedad transita hacia la adopción de esquemas digitales para la prestación de servicios y la realización de actividades cotidianas, por lo cual, el establecimiento de estos esquemas no sólo serán parte de una realidad, sino una necesidad reconocida y demandada por la sociedad. Finalmente, estas estrategias deben ser adoptadas con la finalidad de mantener principios y valores democráticos, sin que su afectación se vuelva una justificación para el uso de esta tecnología.

Fuentes de consulta

Bibliográficas

Mantelero, Alessandro. "Ciudadanía y Gobernanza Digital entre Política, Ética y Derecho". *Sociedad digital y derecho.* Andrés Barrio y José Torregrosa Vázquez (Coord.). Madrid, España, *Boletín Oficial del Estado*, Ministerio de Industria, Comercio y Turismo, 2018, pp. 159-179.

Berg, Chris. *The Classical Liberal Case for Privacy in a World of Surveillance and Technological Change.* Palgrave Macmillan, 2018.

Caravelli, Jack y Nigel Jones. *Cyber security: Threats and responses for government and business*. Santa Barbara, Praeger Security International, 2019, pp. 43-72.

Donaire, J. A. (Ed.) 2017. *Estudios y documentos*. *La compra pública de innovación en la contratación del sector público: Manual práctico.* 1a. edición, Madrid: Instituto Nacional de Administración Pública, 2019.

González Vega, Atenea Romina. *La era de vigilancia de Obama*. México, Universidad Nacional Autónoma de México, 2016.

Delgado, Ana. *Technoscience and Citizenship: Ethics and Governance in the Digital Society,* Springer International Publishing, 2017.

Kosta, Eleni, "Algorithmic state surveillance: Challenging the notion of agency in human rights", *Regulation & Governance.* DOI. https://doi.org/10.1111/rego.12331

Lanza, Edison. "Los principios que garantizan una Internet libre, abierta y inclusiva de todas las personas y grupos sociales" *Gobernanza y regulaciones de internet en América Latina*. Sergio França, Rodrigo Vianna y Thia Mesquita, *(coord.),* Rio de Janeiro, Escola de Direito do Rio de Janeiro da Fundação Getulio Vargas, 2018, pp. 497-515.

Nieva Fenoll, Jordi. *Inteligencia artificial y proceso judicial*. Madrid, Ediciones Jurídicas y Sociales, S.A, 2018.

Pati Prasanthi, Gautam Kumar, Sheo Kumar y Mrutunjaya, "Privacy and Challenges to Data-Intensive Techniques"*, Cyber Defense Mechanisms: Security, Privacy, and Challenges, Cyber defense mechanisms: security, privacy, and challenges.* autam, Saini Dinesh Kumar, Cuong Nguyen Ha Huy (Coords.), Boca Raton, CRC Press, 2021.

Gillespie, Tarleton, "Algorithm", *Digital Works,* Princeton University Press, Princeton, pp. 18-30.

Electrónicas

Mazurowski, Maciej, Buda Mateusz, Saha Ashirbani y Bashir Mustafa. "Deep learning in radiology: An overview of the concepts and a survey of the state of the art with focus on MRI". *Journal of magnetic resonance imaging*, vol. 49, núm. 4, Wiley Online Library, 2019. https://onlinelibrary.wiley.com/doi/epdf/10.1002/jmri.26534 (consultado el 17 de diciembre de 2021).

Hemerográficas

Abdalá, María Belén, Santiago Lacroix Eussler y Santiago Soubie. "La política de la inteligencia artificial: sus usos en el sector público y sus implicancias regulatorias", núm. 185, septiembre 2019, Buenos Aires, Centro de Implementación de Políticas Públicas para la Equidad y el Crecimiento, pp.10-15.

Price, David. "The New Surveillance Normal: NSA and Corporate Surveillance in the Age of Global Capitalism". *Monthly review (New York, N.Y.: 1949),* vol. 66, núm. 3, julio 2014, Nueva York.

Miró, Fernando. "Inteligencia artificial y justicia penal: más allá de los resultados lesivos causados por robots", *Revista de Derecho Penal y Criminología*, núm. 20, 20 de julio 2018, Facultad de Derecho, UNED, 2020, pp. 87–130.