La izquierda mexicana al servicio de la inteligencia artificial (I)

Al parecer la sociedad mexicana y otras tantas en América que buscan valerse de la implementación en gran escala de las tecnologías para resolver problemas de criminalidad y de violencia no lo están entendiendo correctamente

Por: Ricardo Orozco
Globalizacion, 16 de abril 2021

Región: América Latina, Caribe
Tema: Comunicación, Tecnología

El pasado martes 13 de abril, las Comisiones legislativas de Comunicaciones y Transportes y de Estudios Legislativos, del Senado de la República, aprobaron la Minuta con proyecto de decreto por el que se reforman y adicionan diversas disposiciones de la Ley Federal de Telecomunicaciones y Radiodifusión, en materia de Padrón Nacional de Usuarios de Telefonía Móvil.

De acuerdo con lo especificado en la Minuta, el origen de dicha propuesta se encuentra en diciembre del 2020, cuando la Mesa Directiva de la Cámara de Diputados envió el documento al Senado para su estudio y eventual aprobación. La Minuta fue turnada a las Comisiones unidas ese mismo mes, pero fue sólo hasta este abril que la discusión al respecto y el voto de confianza sobre la misma se dio por parte de éstas.

En el debate público nacional, la serie de acontecimientos que rodean a cada paso implicado en la aprobación de dicha reforma ha estado marcada, no obstante, por una legítima y profunda preocupación, por parte de algunos sectores que componen a la población mexicana, debido a que, por un lado, revive el fantasma de los excesos autoritarios de las presidencias de Felipe Calderón (2006-2012) y de Enrique Peña Nieto (2012-2018); y por el otro, a que levanta sospechas y preocupaciones sobre los propósitos de avanzar en la creación de un *padrón nacional de usuarios de telefonía móvil* sustentado en la recolección sus datos biométricos; sospechas y preocupaciones, por lo tanto, y hay que insistir en ello, por completo fundamentadas, dada la experiencia que en México se ha tenido con las prácticas de vigilancia, de control y de espionaje por parte del Estado.

Y es que, en efecto, si hay algo que caracterizó a los dos sexenios pasados, en materia de recolección, almacenamiento, tratamiento y utilización de datos personales de la ciudadanía, en materia de servicios informáticos, radiodifusión y telecomunicaciones, ese algo, en ambos casos, tiene que ver con las prácticas de espionaje que se llevaron a cabo para amedrentar a comunicadores y comunicadoras, intelectuales y defensores y defensoras de derechos humanos (como lo fue el caso, durante la administración de Peña Nieto, del *software Pegasus*, aún pendiente de resolución en la justicia federal) y la filtración, compra y venta de bases de datos con información sensible de la ciudanía (como ocurrió con la venta de la base generada a partir del *Registro Nacional de Usuarios de Telefonía Móvil* — RENAUT, durante el mandato de Calderón).

Esos dos casos, hay que aclararlo, no son los únicos de los que se tenga registro o memoria en el pasado reciente de México. Sin embargo, sí son dos de las experiencias de las más

conocidas por el grueso de la sociedad, dos de las mejor documentadas y dos de las más perniciosas en sus efectos. Pero más aún, si algo caracteriza a ambas eso es el hecho de que su implementación ilegal por parte del Estado mexicano se dio en el marco de un contexto de profunda violencia e inseguridad; contexto, no sobra subrayarlo, en el que el acceso a esas bases de datos, como la del RENAUT; y a ese tipo de *softwares*, como *Pegasus*; por parte de enormes complejos criminales (como los cárteles del crimen organizado) no sólo se ha incrementado sino que, más aún, se ha dado en tales proporciones y con tal pericia en su manejo que, al final del día, en más de una ocasión gobiernos municipales, estatales y nacionales alrededor del mundo se han visto rebasados en sus capacidades de reacción ante los usos delictivos que se les han dado.

Y por si ello no fuese poco, también habría que situar correctamente los usos que por parte de diferentes instancias gubernamentales se les han dado a esas bases y a esos *softwares* dentro del marco de una tradición y de una cultura política profundamente autoritarias que, en el caso de los últimos dos sexenios, se articuló con el desplazamiento político e ideológico del panismo y del priísmo gobernantes hacia extremos cada vez más de derecha, más conservadores e intransigentes con las expresiones sociales de descontento y de resistencia a las imposiciones que sus plataformas de gobierno defendían.

¿No es esa, después de todo, la naturaleza profunda de la guerra en contra del crimen organizado; caballo de batalla personalísimo de Felipe Calderón, pero continuada, aunque sin tanta exposición mediática, por Enrique Peña Nieto?, ¿no ha sido esa guerra algo más que el combate armado, directo, de los complejos entramados del crimen organizado en el país; en tanto que sus principales consecuencias fatales no se hallan en las filas del crimen organizado, sino en los amplios espacios de la vida civil? ¿No ha sido esa guerra, sexenio tras sexenio, el teatro de operaciones que ha justificado los más cínicos y atroces desplantes autoritarios del panismo y del priísmo; escenario, en última instancia, que ha sido utilizado para justificar y legitimar la adquisición, el despliegue, la implementación y el uso sistemático, irrestricto, de cada vez más sofisticados dispositivos de control y de cada vez más *inteligentes* tecnologías de vigilancia, so pretexto de que unos y otras son el pilar de mejores políticas de seguridad, de combate a la delincuencia organizada y de reducción de los índices de violencia en el país?

A panistas, priistas, perredistas y morenistas por igual (junto a todas sus rémoras partidistas), les gusta negar la verdad que se oculta detrás de esas preguntas. Pero la realidad es, a pesar de su cinismo o de su hipocresía, que en cada caso ha sido el argumento del combate a la delincuencia organizada, el pretexto de la reducción de los niveles de violencia experimentados en el territorio nacional, lo que ha conducido a los poderes gobernantes en cada sexenio a subordinar su actuación y a la totalidad de sus estrategias en materia seguridad y de procuración e impartición de justicia a los imperativos y a la lógica de operación de las nuevas tecnologías de la información, basadas en el procesamiento de datos en masa (*data mining*), en el aprendizaje autónomo (*deep learning*) y en la inteligencia artificial.

Y es que, en el fondo, lo que se termina planteando es que las capacidades de recolección de información y de procesamiento de datos con las que cuentan estas tecnologías hacen de ellas instrumentos que sin problemas se hallarían en posibilidades de eficientar el trabajo humano hasta ahora desarrollado y, en última instancia, incrementar sustancialmente la identificación de actos delictivos, acelerar el tiempo de respuesta, garantizar la efectividad de los procesos involucrados, precisar aún más la veracidad de la información recabada para la construcción de las carpetas de los casos y, en consecuencia, casi que en

automático, llegar a un índice superior de sanciones dictadas (condenas efectivas) a los responsables de cometer dichos actos. Las nuevas tecnologías, así, terminan siendo, en y desde esta perspectiva, algo así como el punto de partida de cualquier estrategia de seguridad, de procuración e impartición de justicia y de combate a la violencia que pretenda ser eficiente y efectiva en proporciones poblacionales de masas.

Poco importan en esos argumentos, al parecer, las múltiples consideraciones y evaluaciones que se tendrían que hacer de ellas, sobre todo de carácter ético, en el marco de su implementación. En el momento actual en México, de cara a la instauración del padrón nacional de usuarios de telefonía móvil, no hay en los argumentos que desde el gobierno se esgrimen, por ejemplo, preocupaciones sobre los algoritmos y los códigos fuente de los que se valen estas tecnologías que, en casos específicos de su aplicación, como en las ciudades de Nueva York, Boston y San Francisco, tienden a criminalizar más a personas de piel negra que a personas de piel blanca. Tampoco parece importar la discusión sobre la manera en que este tipo de algoritmos se entrena y aprende por cuenta propia en contextos sociales de profundas desigualdades materiales; situación que ha llevado a experimentar situaciones en las que, de nueva cuenta, los algoritmos terminan criminalizando más a estratos sociales con bajos recursos. Es decir, para ponerlo simple: es inexistente, en la propuesta del gobierno federal sobre esta materia, la preocupación sobre los sesgos sexogenéricos, raciales y de clase sobre los cuales actúan estas tecnologías y a partir de los cuales alimentan su propio aprendizaje.

Bastaría con voltear a ver la manera en que el gobierno chino entrena a sus sistemas de vigilancia para favorecer la criminalización de estratos sociales particularmente incómodos para sus sistema político (como las poblaciones musulmanas) para aprender apenas un par de lecciones básicas sobre los riesgos que conlleva la aplicación masificada de estas tecnologías, supuestamente *inteligentes* y autónomas, sin haber realizado, con antelación, un diagnóstico a profundidad de sus efectos de poder en las capas sociales más explotadas de la sociedad. Más aún, habría que prestar apenas una pizca de atención a los intereses de los capitales que financian sus desarrollos para cobrar conciencia de la manera en que éstas operan para favorecer los procesos de reproducción, acumulación, concentración y centralización de capital ahí en donde se las emplea con base en el argumento de que su utilización responde a necesidades de carácter colectivo, en temas como los de seguridad y justicia.

Al parecer la sociedad mexicana y otras tantas en América que buscan valerse de la implementación en gran escala de este tipo de tecnologías para resolver problemas de criminalidad y de violencia no lo están entendiendo correctamente: la estructura cognitiva en la que se basan los algoritmos de los sistemas de vigilancia que pretenden reducir los índices de una y otra problemática está sustentada en una reestructuración de la vieja lógica del racismo científico, ese mismo que, partiendo del estudio de los cráneos de las personas de color, durante siglos ha justificado que las personas negras tienden, biológicamente, genéticamente, a ser más violentas, más conflictivas, más susceptibles de cometer actos por fuera de la ley y el estado de derecho de una sociedad dada.

Tanto se está avanzando en esta dirección, que ya hay, inclusive, investigaciones avaladas por sociedades científicas *de enorme prestigio* internacional que pretenden cifrar la explicación de la criminalidad en las sociedades contemporáneas a partir del mapeo del genoma humano y la decodificación del ADN de las personas. Es decir, de acuerdo con esta lógica, las personas estarían predeterminadas, por sus genes, su constitución biológica y sus rasgos fenotípicos a ser asesinos seriales, criminales violentos, criminales simples y

comunes, depredadores sexuales, etcétera. Esta agenda, financiada y desarrollada en las grandes economías centrales del sistema internacional en el ámbito de las ciencias genómicas, hay que ser claros y claras al respecto, es la misma que se halla de fondo en los sistemas de vigilancia masiva que se instalan a pasos agigantados en las megalópolis americanas y de otras partes del mundo.

Y es que, después de todo, si el criterio de la valoración de una persona, en cualquier ámbito de la vida en sociedad, está dada por la captura, procesamiento, reconocimiento y análisis de rasgos biológicos y fenotípicos (como lo es el reconocimiento facial) al margen de tal proceder queda toda consideración sobre la personalidad del individuo en cuestión: sus valores, sus procesos metales, su experiencia de vida, sus fundamentos éticos, preferencias políticas, afinidades ideológicas, etcétera. Que los sistemas de inteligencia artificial utilizados por algunos departamentos de policía en Estados Unidos basen sus diagnósticos sobre posibles reincidencias de criminales en el color de su piel o en las medidas de su cráneo, en su complexión física o en los rasgos del rostro es apenas la punta del iceberg de esta nueva amenaza que suponen los algoritmos *autónomos* e *inteligentes*.

Que los desarrollos tecnológicos, por lo menos desde los gérmenes de la revolución industrial del siglo XIX, se producen en términos geométricos antes que a partir de una racionalidad aritmética (esto es, que la más insignificante de las innovaciones supone un *revolucionamiento* no sólo para un rubro en particular, sino para todo un sector, en su totalidad) eso es un hecho incuestionable. Sin embargo, es importante no perder de vista que, a pesar de que la tecnología avanza en esa lógica, para que cada uno de esos hitos que la hace avanzar se produzca, es necesario que las personas que los desarrollan, que los capitales que invierten en ellos y que las máquinas *inteligentes* que surgen de ellos aprendan por un mecanismo de prueba y de error, concentrando enormes cantidades de información para su procesamiento y, a partir de ahí, calcular una serie relativamente amplia, pero finita, de posibilidades y resultados.

Y es que cobrar plena conciencia de ello, en la vida cotidiana de las sociedades, significa, por lo menos, dos cosas. La primera de ellas: que se tienen que romper las barreras que impiden la recolección masiva de información en tiempo real, toda vez que sin los datos que ésta proporciona se hace virtualmente imposible para las maquinas y sus algoritmos *aprender*. Lo segundo es que, mientras se recolecta esa información y se procesan los datos, la maquina y el algoritmo estarían *aprendiendo* y emitiendo resultados en tiempo real, lo que conduce a la enorme proporción de errores o de conclusiones erróneas obtenidas por esta vía para su aplicación en el devenir de las sociedades en las que tienen presencia. Después de todo, en la medida en que las sociedades contemporáneas no dejan de crecer, de volverse más complejas e interdependientes las unas de las otras, la masa de información producida por ellas tiende, proporcionalmente, a ser cada vez más y más cuantiosa.

Es la superación de ese reto, precisamente, lo que explica dos de las tendencias dominantes de nuestra época en lo tocante a la relación entre los humanos y la tecnología de la que se valen para vivir su vida cotidiana. La primera tendencia es, por supuesto, la necesidad de capturar cada vez más aspectos de esa vida cotidiana en el espectro tecnológico; esto es, la imperiosa necesidad de hacer que la vida de las personas dependa cada día más de *softwares* y maquinas *inteligentes* o, por lo menos, equipadas con procesos de recolección de datos que eventualmente terminarán en algún servidor de una corporación transnacional en el ramo (una *BigTech*), so pretexto de seguir perfeccionando el producto tecnológico en cuestión. La segunda tendencia tiene que ver con la concentración y

centralización de toda esa información, pues en la medida en que se tengan más datos almacenados para analizar y procesar los resultados que se obtengan de las operaciones matemáticas realizadas por los algoritmos, se supone, serán más precisos y objetivos.

Incorporación, captura y dependencia de sectores poblacionales cada vez más amplios y diversos en la matriz tecnológica vigente y concentración y centralización de la información generada por esos usuarios y usuarias son dos variables que se corresponden y que se copertenecen porque de la primera depende que la totalidad de la población esté integrada a la matriz tecnológica actual, y de la segunda depende, asimismo, que los datos generados por las personas en su relación con la tecnología sigan alimentando el crecimiento geométrico de los desarrollos tecnológicos y su perfeccionamiento en sus capacidades de vigilancia, de recolección de información, de almacenamiento, procesamiento y análisis de datos; es decir, de ello dependen las condiciones mismas de posibilidad de mejorar los sistemas de control y de dominación colectiva.

Sobre la primera variable, por ejemplo, basta con observar cómo es ella la que explica la popularización y la masificación de productos como los teléfonos *inteligentes*, las pulseras, los relojes y todo tipo de *gadgets* que sirven para contar con un monitoreo permanente, sistemático, ininterrumpido de los hábitos de vida de una persona en el día a día. El famosísimo internet de las cosas, la posibilidad de que un hogar sea inteligente a través de la relación que desarrollan entre si diferentes *gadgets*, conectados por redes 5G o 6G+, es justo eso: la lógica de la integración, captura y dependencia de algún dispositivo tecnológico para desarrollar hasta las tareas más sencillas en la vida de una persona: como prender las luces del hogar, tarea que ahora puede realizar un dispositivo como *Echo*, de *Amazon*. Para apreciar la segunda, no hace falta más que mirar la forma en que las grandes corporaciones dedicadas al rubro de la tecnología de punta avanzan sobre la centralización de cadenas de valor globales a través de su monopolización.

En la medida en que ni una sola persona quede fuera de la matriz tecnológica vigente y en la medida en que toda esa información se concentre y se centralice, el problema de las bases de datos se convierte, precisamente, en eso, en un problema que hay que superar. En sociedades como la mexicana, en la que alrededor de ochenta y seis millones de personas cuentan con un dispositivo celular (de un total poblacional de ciento veintiséis millones de habitantes), las capacidades de penetración de estos dispositivos (más aún si son *inteligentes* y cuentan con conexión esporádica o permanente a internet) ofrecen, sin lugar a dudas, una posibilidad de oro para las *BigTech* con presencia en el país para recabar la información de toda esa población; que no es menor, pues supone alrededor del setenta por ciento del total.

Y es que, incluso si los dispositivos en cuestión no son *inteligentes*, y se reducen al uso tradicional de servicios de transmisión de voz, buzón vocal, conferencia o de mensajería (incluidos los servicios de mensajes cortos), esa información, aunque no avance hacia sus formas más complejas, como las que se producen a partir del uso de aplicaciones móviles, ofrece, por lo menos, una enorme cantidad de datos en lo relativo a geolocalización, tendencias de consumo, hábitos de uso y, cuando se viola la privacidad de las comunicaciones, información relativa a los contenidos de las llamadas y los mensajes. Si a ello se suma, como se pretende hacer a partir de la propuesta votada en las Comisiones del Senado mexicano, la vinculación obligatoria e ineludible de esa información con datos biométricos (como los rasgos faciales o la composición de las huellas dactilares y del iris de los ojos), es factible llegar a un par de conclusiones sobre los riesgos que dicho anclaje supone para las más fundamentales libertades de los ciudadanos y las ciudadanas de este

país.

Poco importa si el proyecto es promovido por la derecha más conservadora y agresiva, como lo fue el panismo calderonista, o si lo hace un proyecto político que se preocupa por avanzar en su agenda de izquierda, como lo es el *morenismo* de la *4T*. En tanto que la lógica de funcionamiento y la constitución estructural del entramado tecnológico no cambie y se sostengan tal y como han sido desarrollados hasta ahora por la fuerza de empuje del capital, los riesgos son mayores que los beneficios.

Ricardo Orozco

Ricardo Orozco: *Internacionalista por la Universidad Nacional Autónoma de México, @r_zco, razonypolitica.org.*

La fuente original de este artículo es Globalización
Derechos de autor © Ricardo Orozco, Globalización, 2021

Comentario sobre artículos de Globalización en nuestra página de Facebook
Conviértase en miembro de Globalización

Artículos de: **Ricardo Orozco**

Disclaimer: The contents of this article are of sole responsibility of the author(s). The Centre for Research on Globalization will not be responsible for any inaccurate or incorrect statement in this article. The Center of Research on Globalization grants permission to cross-post original Global Research articles on community internet sites as long as the text & title are not modified. The source and the author's copyright must be displayed. For publication of Global Research articles in print or other forms including commercial internet sites, contact: publications@globalresearch.ca

www.globalresearch.ca contains copyrighted material the use of which has not always been specifically authorized by the copyright owner. We are making such material available to our readers under the provisions of "fair use" in an effort to advance a better understanding of political, economic and social issues. The material on this site is distributed without profit to those who have expressed a prior interest in receiving it for research and educational purposes. If you wish to use copyrighted material for purposes other than "fair use" you must request permission from the copyright owner.

For media inquiries: publications@globalresearch.ca