Respuesta a cuestionario

"El derecho a la privacidad en la era digital"

Información de la Institución

Comisión de Derechos Humanos de la Ciudad de México (CDHCM)

País: México

Información de contacto: Secretaría Ejecutiva, Tel. + (52) 55.52.29.56.00 Ext. 2402.

secretaria.ejecutiva@cdhcm.org.mx

Fecha: 27 de mayo de 2021.

Antecedentes

La Oficina de la Alta Comisionada de las Naciones Unidas para los Derechos Humanos emitió un llamado para la recepción de contribuciones para su informe temático en materia de privacidad en la era digital. Esta acción da seguimiento, a su vez, al trabajo del *Seminario de Expertas y Expertos sobre Inteligencia Artificial y el Derecho a la Privacidad* ("el Seminario") acaecido el 27 y 28 de mayo de 2020. La Comisión de Derechos Humanos de la Ciudad de México (CDHCM o "la Comisión") presenta sus consideraciones a continuación, con base en las preguntas clave que se proporcionaron.

Key questions and types of input sought

1. **Specific impacts on the enjoyment of the right to privacy** caused by the use of artificial intelligence, including profiling, automated decision-making and machine-learning technologies (hereinafter referred to in short as "**AI**") by governments, business enterprises, international organizations and others. Of particular interest is information concerning:
    a. relevant technological developments, the driving economic, political and social factors promoting the use of AI and the main actors in and beneficiaries of deploying and operating AI (developers, marketers, users);
    b. ways in which AI can help promote and protect the right to privacy;
    c. challenges posed by the use of AI for the effective exercise of the right to privacy and other human rights, including features and capabilities of AI that present existing or emerging problems;
    d. discriminatory impacts of the use of AI;
    e. the interlinkages between the promotion and protection of the right to privacy in the context of the use of AI and the exercise of other human rights (including the rights to health, social security, an adequate standard of living, work, freedom of assembly, freedom of expression and freedom of movement);

La Comisión de Derechos Humanos de la Ciudad de México identifica por lo menos dos áreas de preocupación en torno al uso de inteligencia artificial por parte de los gobiernos -con implicaciones

asociadas en cuanto al rol del sector privado-. Se considera que los siguientes comentarios podrán ser leídos e interpretados a la luz de la información vertida por otros actores especialistas en "el Seminario" sobre el contexto latinoamericano proclive a la desprotección del derecho a la protección de datos personales. Se mencionarán casos en los que hay una aplicación directa de la inteligencia artificial, entendida como cualquier sistema diseñado para realizar tareas que generalmente requerirían inteligencia humana, desde percepción visual hasta toma de decisiones. No obstante, este tipo de acciones debe ser interpretada en un contexto más amplio de desprotección de datos personales, independientemente del uso de la inteligencia artificial. Así, se presentan los siguientes eventos, que conjuntan tanto hechos con intervención de herramientas de inteligencia artificial como hechos que visibilizan la amenaza generalizada hacia la privacidad:

i. En primer lugar, en México existe una tendencia nacional de emisión de política pública y legislación orientada a salvaguardar fines constitucionalmente legítimos mediante la desprotección de datos personales y la injerencia en la vida privada de las personas. Un caso es el de una reforma a la Ley de Instituciones de Crédito que entró en vigor el pasado 23 de marzo de 2021. En ésta, se estableció que aquellas instituciones de banca múltiple o de desarrollo deberán requerir y obtener la geolocalización del dispositivo mediante el cual sus clientes pretendan abrir o utilizar una cuenta bancaria vía digital, con el propósito de evitar el lavado de dinero y el financiamiento al terrorismo. La Comisión emitió un posicionamiento al respecto, en el cual se apuntó la falta de proporcionalidad que constituye este requisito, con afectaciones a los derechos a la privacidad en sentido amplio, la vida privada, a la protección de datos personales, y a la intimidad. Por otra parte, la CDHCM señaló que el consentimiento que se otorga para brindar la geolocalización de una persona se encuentra viciado de origen, en razón de que la alternativa es no acceder a servicios financieros esenciales. También se buscó visibilizar la naturaleza discriminatoria de la medida, pues al condicionar un servicio bancario al hecho de proporcionar la geolocalización -un dato que además potencialmente podría revelar información clave sobre la identidad y cotidianeidad de una persona-, se agudiza el rezago financiero y la brecha digital, especialmente en zonas aisladas de la infraestructura que permite obtener y transmitir este dato.[1]

ii. En segundo lugar, se confirma la tendencia mencionada por la publicación de reformas a la Ley Federal de Telecomunicaciones y Radiodifusión; a través de estas modificaciones, se creó un Padrón Nacional de Usuarios de Telefonía Móvil y se definió la obligatoriedad del registro de toda persona física que cuente con un número de línea telefónica móvil. El registro exige el nombre completo de la persona usuaria, nacionalidad, número de identificación oficial con fotografía, Clave Única de Registro de Población, y datos biométricos. Esta medida fue anunciada en una lógica de combate a ciertos delitos frecuentemente cometidos vía telefónica o con el apoyo de alguno de estos medios. La CDHCM señaló en su momento que no sólo no se plantearon consideraciones de razonabilidad y proporcionalidad en la aprobación de estas reformas, sino que ni siquiera es posible detectar un nexo causal que justifique dichas medidas. [2] Otras preocupaciones al respecto se refieren al rol que jugarán las compañías telefónicas en la obtención y el resguardo de estos datos, dado que las modificaciones normativas no establecen un sistema de vigilancia y control explícitos en el tema. Asimismo, el condicionar la provisión de un servicio -particularmente uno que en la actualidad resulta tan fundamental para la comunicación e incluso el ejercicio de otros derechos, como el trabajo- al hecho de proveer datos de tal sensibilidad, resulta discriminatorio y regresivo en

[1] CDHCM observa con preocupación el aumento de disposiciones que permiten la acumulación de información privada de las personas | Comisión de Derechos Humanos de la Ciudad de México

[2] CDHCM alerta sobre implicaciones de privacidad y datos personales del Padrón Nacional de Usuarios de Telefonía Móvil | Comisión de Derechos Humanos de la Ciudad de México

un contexto de por sí hostil para la privacidad y la protección de datos personales en razón del valor comercial que se les ha asignado en las sociedades contemporáneas.

iii. En tercer lugar, en abril de 2021 resurgió el tema de espionaje por parte del Estado mexicano tras una investigación del periódico de El País que posicionó en el foro público la existencia de cuatro contratos para la adquisición de tecnologías de vigilancia que fueron suscritos por la Fiscalía General de la República (FGR) entre 2019 y 2020.[3] Dichos contratos fueron establecidos con *Neolinx* como empresa intermediaria, la cual también estuvo involucrada en procesos de venta de sistemas de vigilancia a otras autoridades entre 2014 y 2015 (v.g. la Secretaría de la Defensa Nacional, el Centro de Investigación y Seguridad Nacional, la Policía Federal, y la entonces Procuraduría General de la República). La investigación refirió que uno de los contratos se refería a un servicio de localización geográfica marca *Geomatrix* (de la empresa *Rayzone*), el cual permite solicitar este dato de un equipo móvil si se proporciona el número de teléfono o el número de Identidad Internacional de Suscriptor Móvil. A través de este servicio, también se puede establecer un perímetro y solicitar alertas cuando un equipo entre o salga del mismo. En otro de los contratos, se adquirió la plataforma *Echo*, diseñada para la consulta y el análisis de datos masivos. No requiere instalación y no sólo puede obtener información de una persona, sino que puede realizar ciertos tipos de recopilación amplia de todos los usuarios de internet de un territorio amplísimo o, según su propia página de internet, de un país. Uno de los datos que recolecta es la geolocalización.

iv. En cuarto lugar, además de lo que se describe con anterioridad, existe una cultura generalizada de aceptación de este tipo de violaciones a los derechos humanos a la privacidad y protección de datos personales. La CDHCM atendió un caso ilustrativo sobre este asunto mediante su Recomendación 19/2018 *Tratamiento ilegal y arbitrario de datos personales a través de la aplicación "Periscope"*.[4] En un ejemplo de represión digital, que incluyó la recolección de datos personales y transmisión en vivo de elementos de identificación, un funcionario público local -perteneciente a la alcaldía Miguel Hidalgo de la Ciudad de México- realizó operativos para "cazar" vecinos que tiran bolsas de basura; atender un reporte vecinal sobre "ejercicio de prostitución"; y retirar una cadena que obstruía la vía pública". Sin identificarse apropiadamente como autoridad ni advertir la posible difusión masiva de los datos, comenzó a grabar a través de la aplicación *Periscope* al enfrentar a las personas involucradas en los hechos referidos. Destaca el hecho de que algunas de las víctimas pertenecían a grupos de atención prioritaria, i.e. personas con discapacidad y niñas, niños, y adolescentes. Estos actos no sólo tuvieron una recepción mayormente positiva entre las audiencias,[5] sino que manifiestan la complejidad de las intersecciones de derechos que puede implicar el uso de tecnologías digitales: desde el debido proceso hasta el derecho a la intimidad.

v. En quinto lugar, en la misma lógica de la información ya presentada y con el fin de ilustrar el contexto, no necesariamente dependiente del uso de la inteligencia artificial, destaca el caso de la Ley por la que se crea el Banco de ADN para el uso forense de la Ciudad de México, publicada el 24 de diciembre de 2019. A partir de ésta, se creó un Banco de Perfiles Genéticos que almacenará la información asociada a una muestra o evidencia biológica obtenida de personas procesadas penalmente por homicidio, lesiones, privación de la libertad personal

[3] La Fiscalía de México ha contratado en los dos últimos años programas para el espionaje masivo de teléfonos móviles | EL PAÍS México (elpais.com)

[4] Comisión de Derechos Humanos de la Ciudad de México. Recomendación 19/2018 *Tratamiento ilegal y arbitrario de datos personales a través de la aplicación "Periscope"*, https://cdhcm.org.mx/wp-content/uploads/2018/12/reco_1918..pdf

[5] Llaman la atención los comentarios en algunas de las publicaciones. *Cfr.* #VecinoCochino y #VecinoGandalla en Jacarandas Bosques de las Lomas #MHestuCasa - YouTube

con fines sexuales, incesto, secuestro, violación, estupro, privación ilegal de la libertad, y feminicidio-. Aunque éste aún no se implementa, configura una amenaza directa al uso razonable, proporcional, y objetivo de datos personales en específico por la falta de regulación del propio banco de datos y su uso.

vi. Finalmente, en abril de 2021 se instauró un Registro Público de Personas Agresoras Sexuales[6] de la Ciudad de México, como resultado de reformas a la Ley de Acceso de las Mujeres a una Vida Libre de Violencia de esta entidad federativa y legislación asociada -como el Código Penal local-. En éste, se expone el nombre completo, la edad, la nacionalidad, y, en muchos casos, la imagen de personas sentenciadas por feminicidio, violación, turismo sexual, trata de personas, o delitos contra menores de 12 años (específicamente violación, abuso sexual, o acoso sexual). En la discusión pública, se ha asignado un capital político significativo a estas dos medidas bajo la justificación del combate a la violencia en contra de las mujeres. No obstante, la CDHCM observa que facilitan un amplio proceso de revictimización y desprotección de los datos personales de las personas registradas, bajo criterios discriminatorios en contra de las personas privadas de la libertad. Llama la atención además que existen criterios de la Primera Sala de la Suprema Corte de Justicia de la Nación que diferencian aquellos casos en los que la publicación de datos personales sería proporcional y razonable -especialmente cuando se busca a una persona sustraída de la acción de la justicia-;[7] en contraste, el Registro Público de Personas Agresoras Sexuales contradice directamente esta lógica al ser personas que ya cumplen su sentencia.

Con base en lo anteriormente descrito, la CDHCM identifica, por lo menos, dos tipos de impacto: por un lado, las amenazas a la privacidad que configuran algunas medidas legislativas y de política pública que no son vigentes aún y, por otro, las violaciones del derecho a la privacidad configuradas a partir de medidas ya implementadas.

En ambos casos, se prevé el reto de monitorear estrictamente la actuación judicial. Por ejemplo, en el caso del Padrón Nacional de Usuarios de Telefonía Móvil, éste fue recientemente impugnado mediante una acción de inconstitucionalidad por el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), un órgano constitucional autónomo, por considerarse violatorio a los derechos de protección de datos personales y de acceso a la información.

En cuanto al Registro Público de Personas Agresoras Sexuales, esta misma Comisión interpuso también acciones de inconstitucionalidad tanto en la Suprema Corte de Justicia de la Nación como en la Sala Constitucional del Poder Judicial de la Ciudad de México. De esta forma, la autoridad jurisdiccional deberá presentar argumentación conforme a los estándares constitucionales y convencionales en materia de derecho a la privacidad, dado que es probable que estas decisiones sienten bases importantes para la interpretación posterior no sólo en este tema, sino en la utilización de inteligencia artificial para acumular y analizar datos.

El otro reto que se identifica tiene que ver con la actuación jurisdiccional en materia de reparaciones: incluso si se determinara la inconstitucionalidad de un instrumento como el Registro Público de Personas Agresoras Sexuales, deberá garantizarse la reparación integral del daño ejercido en contra de las víctimas. Esto podría ser también aplicable al asunto de la geolocalización exigida en la Ley de Instituciones de Crédito. En general, el Poder Judicial tendrá próximamente en su coto la posibilidad

[6] Registro Público de Personas Agresores Sexuales de la CDMX

[7] Tesis 1a. VI/2021 (10a.) FICHAS DE BÚSQUEDA DE PERSONAS SUSTRAÍDAS DE LA ACCIÓN DE LA JUSTICIA EMITIDAS POR AUTORIDAD MINISTERIAL. SU PUBLICACIÓN CON LOS DATOS GENERALES, EL NOMBRE Y LA FOTOGRAFÍA DE LOS SUJETOS BUSCADOS PARA EJECUTAR UNA ORDEN DE APREHENSIÓN, NO VIOLA EL DERECHO A LA PRIVACIDAD. Gaceta del Semanario Judicial de la Federación. Libro 84, Marzo de 2021, Tomo II, página 1228, https://sjf2.scjn.gob.mx/detalle/tesis/2022831

de reivindicar el derecho a la privacidad en más de un sentido: a través del marcaje constitucional de lo que el sistema puede permitir sin impedir el goce de los derechos humanos y por medio de reparaciones idóneas y proporcionales.

2. **Legislative and regulatory frameworks**, including:
    a. information on relevant existing or proposed national and regional legislative and regulatory frameworks and oversight mechanisms;
    b. analysis of related human rights protection gaps, ways to bridge those gaps and barriers to advancing effective, human-rights based regulation of AI;
    c. assessments of the need to prohibit certain AI applications or use cases ("red lines").

El marco de protección al derecho a la privacidad en el entorno digital está mayoritariamente contenido en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y sus correlativas en cada entidad federativa.

Al respecto de los asuntos que se señalan en el presente texto y que comprometen el derecho a la privacidad de las personas, se hace referencia al Registro de Usuarios de Telefonía Móvil recientemente incorporado en la Ley Federal de Telecomunicaciones y Radiodifusión (180 Bis a 180 Séptimus), así como al Registro de Personas Agresores Sexuales incorporado en la Ley de Acceso a las Mujeres a una Vida Libre de Violencia de la Ciudad de México; y la Ley por la que se Crea el Banco de ADN para uso Forense en la Ciudad de México, respecto del cual existe la preocupación de que su implementación no reproduzca las fallas estructurales en materia forense, seguridad de los datos y protección de las víctimas que los otorgan.