



# LATIN AMERICA

IN A GLIMPSE



Este informe fue realizado por Derechos Digitales

Editado por Vladimir Garay.  
Diseño y diagramación por Constanza Figueroa.  
Corrección de estilo por Rocío Consales.

Enero 2020.

Esta obra está disponible bajo licencia Creative Commons Attribution 4.0 Internacional (CC BY 4.0): <https://creativecommons.org/licenses/by/4.0/deed.es>



## CAPÍTULO 1

# RECUPERANDO, APROPIANDO Y APRENDIENDO FEMINISMO Y TECNOLOGÍA EN AMÉRICA LATINA

Por Juliana Guerra

A fines de marzo en México, una ola de denuncias sobre acoso y abuso sexual comenzó a circular a través de Twitter. Las primeras acusaciones surgieron de un sondeo realizado por Periodistas Unidas Mexicanas,<sup>1</sup> pero rápidamente se viralizó a otros gremios. Escritores, académicos y activistas comenzaron a ser denunciados con nombre y apellido junto a la etiqueta #MeTooMx y otros *hashtag* similares.

Esta ola de denuncia se sumó a otras anteriormente ocurridas en Costa Rica, El Salvador y Guatemala,<sup>2</sup> que a su vez retomaban la iniciativa surgida en Estados Unidos un año atrás. Pero si este movimiento es una muestra de fuerza, resistencia y resiliencia por parte de las denunciantes,<sup>3</sup> también ha sido detonante de nuevas violencias, algunas sutiles<sup>4</sup> y otras fuertes e implacables. Ante esta amenaza re victimizante, ha sido muy importante la defensa del anonimato<sup>5</sup> y las reflexiones sobre las formas de justicia feminista que este tipo de acciones busca.<sup>6</sup>

La violencia de género y la discriminación en línea no son más que extensiones de una situación estructural de exclusión, cuya eliminación requieren transformaciones en los distintos escenarios que forman el ecosistema sociotécnico que da forma a internet. En América Latina, desde hace varios años se viene fortaleciendo un movimiento que, desde una postura feminista, está intentando generar esos cambios. No es un movimiento homogéneo ni centralizado, pero está cada vez más articulado frente a la necesidad común de erradicar el riesgo que atenta contra las libertades individuales y colectivas, tanto de las mujeres como de otros grupos cuyas identidades de género son marginadas, estigmatizadas y sujetas a distintas formas de violencia. La edición 2017 de *Latin America in a Glimpse*<sup>7</sup> centraba la mirada precisamente en aquellas iniciativas que conjugaban género y tecnología de maneras diversas, críticas, desafiantes y siempre

1 <https://www.animalpolitico.com/2019/03/metoo-periodistas-mexicanos-mujeres-denuncian-acoso-medios/>

2 <https://www.pikaramagazine.com/2019/07/metoo-centroamerica/>

3 <https://www.derechosdigitales.org/13082/interfaces-para-la-accion-colectiva/>

4 <https://girlanachronism.org/>

5 <https://luchadoras.mx/metoo-el-anonimato-se-defiende/>

6 <https://genderit.org/node/5335>

7 [https://www.derechosdigitales.org/wp-content/uploads/glimpse2017\\_spa.pdf](https://www.derechosdigitales.org/wp-content/uploads/glimpse2017_spa.pdf)

interesantes. Hoy, dos años más tarde y de forma más breve, volvemos sobre los esfuerzos que se están realizando en la región para contrarrestar los efectos de las violencias sobre los cuerpos y las vidas de quienes la enfrentan.

En enero se publicó en México La Clika,<sup>8</sup> una novela gráfica web para hablar sobre la violencia en línea, reconociendo que *es virtual y es real* y que *no es culpa* de quien la enfrenta. La plataforma, desarrollada en conjunto por Luchadoras<sup>9</sup> y La Sandía Digital,<sup>10</sup> ofrece alternativas para responder a la difusión no consentida de imágenes íntimas, así como herramientas de autodefensa digital para prevenir y contrarrestar otros tipos de violencia relacionada con la tecnología.

*La brecha de género en internet es también un problema de acceso. No se trata solo de los bajos niveles de escolaridad femenina en carreras de ciencia y tecnología, las barreras de participación en la industria o la diferencia salarial; se trata de todo un sistema que, a través de explicaciones biologicistas, desincentiva en las mujeres el interés por estos temas.*

En marzo se lanzó Vita Activa,<sup>11</sup> una línea de apoyo vía chat en Whatsapp, Signal y Telegram, donde se brinda asesoría legal y psicológica a las mujeres que sufren violencia en las redes. Su propuesta consiste en dar recomendaciones para recuperar la estabilidad emocional, informar sobre las posibilidades de acción frente a la situación que se está enfrentando y acompañar en la toma de decisiones. En junio se lanzó también el bot de Acoso.Online,<sup>12</sup> un sistema automatizado con criterios feministas que, a través de Telegram, ofrece información tanto a las víctimas como a su círculo cercano sobre cómo enfrentar un caso de difusión no consentida de imágenes íntimas en internet.

En julio, la organización paraguaya Tedic<sup>13</sup> publicó data.cuenta,<sup>14</sup> un test para reconocer, visibilizar y medir experiencias de violencia mediadas por la tecnología. La plataforma es dirigida principalmente a estudiantes de secundaria y universidad y contiene un glosario con las diferentes formas de violencia, un directorio de organizaciones, colectivas e

iniciativas que ofrecen contención jurídica, psicológica y emocional, así como también recomendaciones legales de acuerdo con la legislación paraguaya y tratados internacionales. Su código está abierto y disponible<sup>15</sup> para ser replicado en otros países.

Por su parte, el Encuentro Nacional de Mujeres -que se celebra anualmente desde 1986 en Argentina-<sup>16</sup> convocó a más de 80.000 mujeres en la ciudad de La Plata a finales de octubre y, por primera vez, incluyó la organización de una comisión de seguridad que puso a disposición de las asistentes la app “AUTOCUIDADO 34 Encuentro” con recomendaciones de cuidado colectivo, mapas, teléfonos y lugares donde pedir ayuda en caso de alguna situación de riesgo.<sup>17</sup> La app, y en general el trabajo de la comisión, busca hacer frente a la represión policial y al hostigamiento por parte de los grupos anti derechos, que en años anteriores han atacado violentamente no solo al Encuentro, sino también a otras movilizaciones como las del 8 de marzo, #NiUnaMenos o la Marea Verde, entre otras.

Junto con ello, y también por vez primera, el encuentro abrió un taller sobre ciberfeminismo e inclusión

8 <https://www.libresenlinea.mx/>

9 <https://luchadoras.mx/>

10 <http://lasandiadigital.org.mx/>

11 <https://vita-activa.org/>

12 <https://acoso.online/cl/chat-de-ayuda/>

13 <https://cyborgfeminista.tedic.org/amigue-date-cuenta/>

14 <https://datacuenta.tedic.org/>

15 <https://gitlab.com/tedicpy/data.cuenta>

16 <http://encuentrodemujeres.com.ar/historia-del-encuentro/>

17 <https://www.pagina12.com.ar/222467-una-app-de-seguridad-para-el-encuentro-nacional-de-mujeres-e>

digital<sup>18</sup> a cargo de la Fundación Activismo Feminista Digital,<sup>19</sup> donde se habló de la violencia estructural que, sumada a la brecha digital de género, se traduce en la censura a las expresiones de las mujeres en internet. Además de las herramientas de respuesta ante situaciones de violencia, estos espacios de aprendizaje han sido una estrategia continuada durante los últimos años y han permitido a las personas tomar medidas preventivas, así como tener mayor conciencia sobre los riesgos y amenazas que conlleva el uso de la tecnología, pero también sobre las posibilidades que ofrecen tanto internet como las redes humanas de apoyo.

Durante 2019 destacamos la apertura de Tecnoresistencias: centro de autodefensa digital en Perú,<sup>20</sup> un espacio para brindar herramientas legales, digitales y sociales de cuidado y defensa a quienes constantemente enfrentan violencia en línea, desde una perspectiva de género, interseccional y de derechos humanos. Tecnoresistencias se ha aliado con distintas colectivas feministas a nivel local para la realización de talleres y procesos de acompañamiento en estos temas. También destacamos el trabajo realizado por la colectiva Hackeando al machismo en Bolivia, que desde 2018 comenzó un proceso de aprendizaje y adopción de prácticas de cuidado digital, como complemento a acciones directas de denuncia frente a la situación generalizada de violencia de género que se vive en el país. Hackeando al machismo, además, apoyó la realización de la segunda FemhackPartyLAC,<sup>21</sup> evento paralelo al Foro de Gobernanza de Internet de América Latina, que en 2019 tuvo lugar en La Paz, a principios de agosto.

## Recuperando espacios y apropiando las tecnologías

La lucha por la eliminación de las violencias de género en internet ocupa un lugar importante en el trabajo que muchas colectivas y organizaciones hacemos a diario. Así mismo cada vez hay más iniciativas<sup>22</sup> que promueven acciones afirmativas para cerrar las brechas y dejar sin lugar a los sesgos y la discriminación.

A mediados de julio en el estado de Chiapas, México, se reunieron 25 mujeres en un encuentro hackfeminista a reflexionar desde el hacer<sup>23</sup> y trabajar por una tecnología de los afectos y la (co)responsabilidad. Una conclusión central de ese encuentro fue la necesidad de construir una internet feminista, rompiendo con el conocimiento experto y creando “una red local que nos permita hacer una internet digna para nosotras y nuestros territorios”.<sup>24</sup>

También en julio, y por tercer año consecutivo, se celebró la Hackerfem!<sup>25</sup> en Paraguay, la fiesta de mujeres en tecnología que en esta edición convocó a más de 90 compañeras para celebrar y compartir sobre proyectos, trabajos, ideas y hobbies desde distintos sectores y experiencias. Además, a comienzos de septiembre, en Costa Rica se celebró una nueva edición de LatINiTY,<sup>26</sup> la conferencia de mujeres latinoamericanas apasionadas por las tecnologías digitales. Este evento, organizado por la Cooperativa Sulá Batsú<sup>27</sup> y su programa TICas, se propuso este año hacer un análisis crítico sobre el papel de la tecnología en la región, así como proponer soluciones a los principales retos y riesgos de la sociedad digital.

En agosto en Buenos Aires, Argentina, se celebró NotPinkCon, una conferencia sobre seguridad informática, con enfoque técnico, de entrada libre y gratuita e impartida exclusivamente por mujeres. Su objetivo es incentivar la participación de más mujeres en el campo y brindar un espacio más cómodo para compar-

18 <https://www.0221.com.ar/nota/2019-10-13-16-44-0-acoso-censura-y-activismo-cibernetico-la-mirada-2-0-de-un-flamante-taller-del-encuentro>

19 <https://activismofeministadigital.org/>

20 <https://hiperderecho.org/tecnoresistencias/>

21 <https://www.genderit.org/es/feminist-talk/vamos-hackear-internet-juntas-2do-femhackparty-lac>

22 <https://www.articaonline.com/2019/07/internet-feminista-y-conocimiento-libre/>

23 <https://latinta.com.ar/2019/08/hackerfeminismo-afectadas-y-afectando-desde-las-tecnologias/>

24 <https://sursiendo.org/blog/2019/07/encuentro-hackfeminista-en-chiapas-estar-en-analogico-para-construir-entornos-digitales-mas-dignos-para-nosotras/>

25 <https://cyborgfeminista.tedic.org/hackerfem-2019-recuento-de-nuestras-dos-jornadas-de-apropiacion-tecnologica-y-aprendizaje-en-comunidad/>

26 <https://latinitycr.com/>

27 <https://www.sulabatsu.com/>

tir sus investigaciones sobre un tema que ha sido tradicionalmente dominado por hombres.<sup>28</sup> También en Argentina, Las de Sistemas continúan fortaleciéndose como comunidad feminista en la industria técnica, visibilizando y potenciando el trabajo de mujeres, lesbianas, trans y no binaries. Este año participaron también del 34° Encuentro Nacional de Mujeres<sup>29</sup> para fortalecer redes de trabajo y apoyo en temas diversos, y organizaron la segunda versión de FemIT,<sup>30</sup> conferencia que realizan en su segundo aniversario para compartir conocimientos técnicos, abrir debates sobre género y tecnología y visibilizar el trabajo de los grupos e identidades minoritarias en este campo.

Y es que la brecha de género en internet es también un problema de acceso.<sup>31</sup> No se trata solo de los bajos niveles de escolaridad femenina en carreras de ciencia y tecnología, las barreras de participación en la industria o la diferencia salarial entre hombres y mujeres, que para 2019 en Argentina es del 14.55%;<sup>32</sup> se trata de todo un sistema que, a través de explicaciones biologicistas, desincentiva en las mujeres el interés por estos temas, mientras que en los espacios de desarrollo académico y profesional, mayoritariamente masculinos, se reproducen y promueven comportamientos patriarcales, discriminatorios y violentos.<sup>33</sup>

*No es un movimiento homogéneo ni centralizado, pero está cada vez más articulado frente a la necesidad común de erradicar el riesgo que atenta contra las libertades individuales y colectivas, tanto de las mujeres como de otros grupos cuyas identidades de género son marginadas, estigmatizadas y sujetas a distintas formas de violencia.*

### Moldeando territorios e infraestructuras

Pero la discriminación de género no es un problema solo de la industria, también de los movimientos sociales. Por eso surgió Geochicas,<sup>34</sup> una iniciativa de mujeres colaboradoras de Open Street Map,<sup>35</sup> reunidas con el objetivo visibilizar la desigualdad de género y el acoso dentro de la misma comunidad de Open Street Map. Entre otros proyectos que han desarrollado desde su creación en 2016, en 2018 comenzaron a construir colaborativamente un mapa de las calles con nombre de mujer en ciudades de América Latina y España,<sup>36</sup> para visibilizar la brecha que existe en la representación de figuras femeninas. Además de ofrecer información sobre el porcentaje de calles con nombres de mujeres con respecto a las calles con nombres de hombre, el mapa indica cuántas de estas mujeres aparecen reseñadas en Wikipedia y por eso, además de promover el mapeo de calles, el proyecto incentiva y abre espacios para la edición colaborativa de las biografías de estas mujeres.

Vale decir que para 2018, no más del 5% de las personas que contribuyen con Open Street Map, y no más del 9% de quienes contribuyen con Wikipedia, son mujeres.<sup>37</sup> Pero más allá de las cifras, hay múltiples formas de opresión que enfrentan las mujeres en los entornos tecnológicos, llámese empresas, organizaciones o redes comunitarias.<sup>38</sup> Aunque las características de estos espacios sean muy distintas, las condiciones de opresión son una constante, tanto para las mujeres como para personas con identidades de género diversas, personas con niveles de escolaridad bajos, personas de color, indígenas, habitantes rurales o adultas mayores. Opciones que es necesario visibilizar y nombrar, al tiempo que se construyen alternativas.

28 <https://notpinkcon.org/>

29 <https://www.marcha.org.ar/en-el-mundo-de-unos-y-ceros-vamos-por-la-diversidad/>

30 <http://lasdesistemas.org/>

31 <https://adc.org.ar/2019/08/30/por-que-la-desercion-de-las-mujeres-en-las-tic-es-un-problema-de-acceso/>

32 <https://openqube.io/encuesta-sueldos-2019.02#Genero-Progresion-historica-Historico-de-nivel-de-participacion>

33 <https://www.technologyreview.es/s/11227/como-romper-el-techo-de-silicio-que-oprime-las-mujeres-en-tecnologia>

34 <https://geochicas.org/>

35 <https://www.openstreetmap.org/>

36 <https://geochicasosm.github.io/lascallesdelasmujeres/>

37 <https://blog.mapillary.com/update/2019/05/28/putting-women-on-the-map-with-geochicas.html>

38 <https://genderit.org/es/feminist-talk/edicion-especial-viaje-ilustrado-de-mujeres-por-las-redes-comunitarias>

7

Las comunidades de desarrollo exclusivas son una opción, como es el caso de AfroPython en Brasil,<sup>39</sup> un taller dirigido a personas negras para incentivar su interés en la programación. También el empleo exclusivo, como en el caso de Trans-Ti,<sup>40</sup> una start up argentina que contrata exclusivamente personas travesti y trans, así como las asociaciones y cooperativas de autoempleo de grupos vulnerables.<sup>41</sup> Otra opción es la creación de protocolos feministas para el diseño e implementación de sistemas informáticos, como ha hecho el programa TIC-as en Centro América<sup>42</sup> o la incidencia en el diseño de protocolos para la infraestructura de internet, como hemos venido haciendo desde Derechos Digitales y Artículo 19.<sup>43</sup>

Otras alternativas se concentran en garantizar la soberanía de los espacios donde se aloja nuestra información. Desde garantizar mayor transparencia y acompañamiento al ofrecer servicios o promover el desarrollo de habilidades técnicas para un mejor y más informado uso de los recursos, hasta disponer de la información necesaria, de una manera clara y accesible, para montar redes locales propias, como propone el proyecto Fuxico<sup>44</sup> o para montar servidoras transhackfeministas en la casa, como propone La Bekka.<sup>45</sup> En cualquiera de estos casos, el trabajo está centrado en que la tecnología sirva para fortalecer y alimentar redes humanas, en ningún caso al revés. Esa es la apuesta feminista que permea todo lo anteriormente expuesto.

---

39 <https://afropython.org/>

40 <https://trans-ti.com/>

41 <https://genderit.org/es/articles/edicion-especialcooperativas-para-la-reapropiacion-sustentable-de-tecnologias-y-redes-de>

42 Presentación en el marco de Citizenlab Summer Institute, Toronto 2019.

43 <https://www.derechosdigitales.org/12908/protocolos-para-una-internet-libre-y-segura/>

44 <https://www.fuxico.org/>

45 <https://labekka.red/novedades/2019/11/05/lanzamiento-fanzine.html>

## CAPÍTULO 2

# MAL DE OJO

## RECONOCIMIENTO FACIAL EN AMÉRICA LATINA

Por Vladimir Garay

“Me podrían haber arruinado la vida; a mí y a mi familia”.<sup>1</sup> Esa es la reflexión que hace Guillermo Ibarrola frente a la cámara de A24, tras ser puesto en libertad después de estar seis días detenido por un crimen que no cometió, víctima de una pesadilla tecno-kafkiana.

Mientras se encontraba en Retiro, la principal terminal de omnibuses de Buenos Aires, dos policías se acercaron a Ibarrola y lo detuvieron. El sistema de reconocimiento facial que desde abril de 2019 opera en la capital argentina lo había identificado como responsable de un robo ocurrido en 2016 en Bahía Blanca.

Pero Ibarrola nunca había estado en Bahía Blanca ni tampoco había participado de ningún delito. El sistema había cometido una equivocación que solo fue enmendada seis días más tarde, mientras estaba siendo trasladado a una cárcel provincial. Mientras se encontraba detenido, Ibarrola intentó explicar que debía tratarse de un error. No importó, la máquina había dado ya un veredicto.

La implementación de sistemas de identificación biométrica -y particularmente de reconocimiento facial- ha sido uno de los puntos más debatidos durante los últimos años en la intersección entre tecnología y derechos fundamentales. Las promesas de exactitud, precisión y diligencia con las que se ha querido promocionar este tipo de tecnologías ha encontrado varias respuestas favorables entre los gobiernos y entidades estatales en América Latina, que suelen publicitar con gran pompa los esfuerzos realizados por incorporar estas técnicas a sus actividades, como símbolo de modernización.

Sin embargo, la experiencia internacional ha mostrado que las tecnologías de reconocimiento facial conllevan una serie de problemáticas difíciles de sortear y que las autoridades rara vez mencionan a la hora de anunciar públicamente la intención de poner en funcionamiento un sistema de este tipo. A la dificultad inherente a proteger debidamente datos altamente sensibles como los biométricos, se suma el alto porcentaje de falsos positivos arrojado por distintos sistemas de reconocimiento facial en funcionamiento alrededor del mundo, particularmente cuando se trata de personas de tez oscura, personas trans o no binarias.

En un experimento realizado por la American Civil Liberties Union (ACLU) el software de reconocimiento facial desarrollado por Amazon reconoció erróneamente a 28 congresistas estadounidenses como autores de algún crimen, con un número desproporcionadamente alto de personas de color entre ellos.<sup>2</sup> El

<sup>1</sup> Más información en <https://www.pagina12.com.ar/209910-seis-dias-arrestado-por-un-error-del-sistema-de-reconocimien>

<sup>2</sup> Más información en <https://www.aclu.org/blog/privacy-technology/surveillance-technologies/amazons-face-recognition-falsely-matched-28>

proyecto Gender Shades,<sup>3</sup> desarrollado por la investigadora Joy Buolamwini, demuestra que las tecnologías de reconocimiento facial disponibles en el mercado tienen grandes dificultades identificando mujeres de color, y obtienen sus mejores resultados cuando los sujetos analizados son hombres blancos.

Al mismo tiempo, la promesa de un sistema de reconocimiento facial completamente eficaz –imposible como es– no evoca precisamente un escenario idílico, sino más bien una distopía orwelliana, donde cada movimiento puede ser observado, registrado y escudriñado. Es por ello que, en una de sus editoriales, el periódico inglés *The Guardian* catalogó al reconocimiento facial como un peligro para la democracia<sup>4</sup> y cuatro ciudades estadounidenses –Oakland, San Francisco Berkeley y Somerville, Massachusetts– la han prohibido.<sup>5</sup>

A todos los problemas anteriormente mencionados, en América Latina se suma un actuar muchas veces opaco y una interpretación antojadiza de leyes que no fueron concebidas para lidiar con las implicancias de este tipo de tecnologías, configurando un escenario de altas incertezas y muchas zonas grises, particularmente en relación con la defensa de los derechos fundamentales de las personas sometidas a estos sistemas. Estos problemas se agudizan cuando la tecnología es utilizada en tareas relativas a la persecución criminal y el orden público, donde la información muchas veces se vuelve inaccesible, escudada bajo leyes de seguridad nacional que le permiten funcionar sin control. Al respecto, los casos de Paraguay y Argentina son ilustradores.

En marzo de 2019, el Gobierno de la ciudad de Buenos Aires anunció la implementación de un sistema de reconocimiento facial para detectar prófugos y rebeldes de todo el país. Se trata de una nueva adhesión al sistema de biovigilancia pública de la ciudad, que ya contaba con una extensa red de cámaras, a algunas de las cuales se les ha adosado un software de reconocimiento facial, particularmente aquellas dispuestas en terminales y estaciones del tren subterráneo, el Subte.

“Sabemos que son alrededor de 200 cámaras que están usando ese software. El Gobierno no dice en qué estaciones están ni en qué cámaras están dentro de se subte. Desde ADC hicimos un pedido de acceso a la información para que nos informen eso y nos negaron esa información en base a razones de seguridad”, explica Eduardo Ferreyra de la Asociación por los Derechos Civiles (ADC).

Algunas de las materias incluidas en el acceso a la información pública realizado por ADC dicen relación con la legalidad de la iniciativa y los protocolos de control que lo rigen, los aspectos técnicos del sistema y la composición de la base de datos utilizada. En opinión de la organización, las respuestas no fueron suficientemente precisas.<sup>6</sup>

El caso paraguayo es similar. Desde mediados del año pasado, el centro histórico de Asunción, el aeropuerto de la ciudad y las terminales de buses está siendo vigiladas por un sistema de reconocimiento facial donado por la Comisión Nacional de Telecomunicaciones (CONATEL) al Ministerio del Interior. “El ente regulador de comunicaciones tiene un fondo, que se llama Fondo Universal, que es exclusivamente para conectividad. Y, extrañamente, lo están utilizando para compras de seguridad y donando a otras instituciones del Estado, a través de convenios interinstitucionales”, explica Maricarmen Sequera, directora ejecutiva de TEDIC.

Puesto que CONATEL no forma parte del convenio de contrataciones públicas, la licitación se realizó de forma cerrada. Ante la total oscuridad con la que se estaba operando, TEDIC interpuso un recurso de acceso a la información pública con una serie de preguntas respecto al funcionamiento del sistema, incluyendo la geocalización de las instalaciones, la base de datos utilizada y también respecto a la evaluación de impacto previa.

3 Disponible en <http://gendershades.org/>

4 Disponible en <https://www.theguardian.com/commentisfree/2019/jun/09/the-guardian-view-on-facial-recognition-a-danger-to-democracy>

5 Más información en <https://gizmodo.com/berkeley-becomes-fourth-u-s-city-to-ban-face-recogniti-1839087651>

6 Toda la información sobre el requerimiento se puede revisar en <https://adcdigital.org.ar/2019/05/23/con-mi-cara-no-reconocimiento-facial-en-la-ciudad-de-buenos-aires/>

“La respuesta a esa solicitud de acceso fue parcial -advierte Sequera- Nos pasaron cierta información, pero era información que a la que ya habíamos accedido y no realmente sobre las preguntas que hicimos. Entonces apelamos y en la primera instancia el Ministerio del Interior dice que la otra información no la pueden dar por cuestiones de seguridad nacional”.

Sin embargo, la ley paraguaya establece que para que una información sea reservada debe ser expresamente establecida por ley, no siendo este el caso. “Metieron este tema dentro de una mesa de seguridad nacional que tiene el Sistema de Inteligencia y con eso justificaron que todo lo que se discuta ahí es de seguridad nacional. Apelamos, y en la segunda instancia de nuevo los tres jueces aprobaron la posición del ministerio del interior, sin argumento”,<sup>7</sup> declara Sequera.

Esta reticencia a transparentar información relativa al funcionamiento de los sistema de reconocimiento facial es preocupante, pues, como acota Leandro Ucciferri en un texto a propósito de la solicitud de transparencia realizado por ADC, “El reconocimiento facial, en particular cuando se lo usa con fines de investigación

criminal, tiene el potencial de interferir directamente con derechos como la privacidad, la libertad de expresión, reunión y asociación, la no discriminación y garantías constitucionales como el debido proceso y la presunción de inocencia”.

La falta de disposición para entregar información de cuestiones tan básicas como los proveedores de la tecnología que se está utilizando impide incluso hacerse una idea general respecto a la calidad de la herramienta en uso. Y es que no todos los sistemas de reconocimiento facial son iguales: las pruebas realizadas por la Metropolitan Police de Londres entre 2016 y 2018 arrojaron una tasa de falsos positivos del 96%.<sup>8</sup> Si alguna iniciativa local considerara usar la misma tecnología sería importante saberlo.

En ese sentido, el caso boliviano es diferente. Presentado a fines de agosto y catalogado por el Ministro de Gobierno,

Carlos Romero, como el programa de seguridad ciudadana más moderno de todo el continente,<sup>9</sup> Bol-110 es un ambicioso proyecto de adquisición de tecnologías de vigilancia “que van a estar en todo: en escuelas, taxis, hospitales”, explica Hugo Miranda de Internet Bolivia.

Aquí, la tecnología está a cargo de la empresa estatal china CEIEC, responsable también de la infraestructura del programa ECU-911<sup>10</sup> en Ecuador. Coincidentemente, el financiamiento viene también por parte del Banco Nacional de China, Eximbak, que facilitó a Bolivia la suma de 105 millones de dólares para poner en marcha Bol-110.<sup>11</sup> Y aunque el proyecto no alcanzó a ser aprobado por el Poder Legislativo antes de la elección presidencial del 20 de octubre, los equipos ya fueron adquiridos.

“No es regular, no debería haber sucedido algo así, porque no tiene sentido comprar equipos que luego no se sabe cómo se van a utilizar. Pero como la voluntad estaba depositada sobre todo en el financiador, entonces pueden comenzar a hacer los procesos y luego darse cuenta de que necesitan un marco legal; me da la impresión de que eso es lo que ha sucedido. Probablemente incluso – estoy ahora especulando – había una necesidad de comprar en esta gestión esos equipos. Y, paralelamente, han ido proyectando la ley; y eso,

7 Toda la información relativa a los requerimientos de acceso a información pública se encuentran en <https://www.tedic.org/quien-vigila-al-vigilante-reconocimiento-facial-en-asuncion/>

8 Más información en <https://www.independent.co.uk/news/uk/home-news/facial-recognition-london-inaccurate-met-police-trials-a8898946.html>

9 En <https://www.youtube.com/watch?v=IAW3I8Dfngw>

10 Más información en <https://www.nytimes.com/es/2019/04/24/ecuador-vigilancia-seguridad-china/>

11 Más información en <https://m.eldiario.net/?n=65&a=2017&m=01&d=11>

*La promesa de un sistema de reconocimiento facial completamente eficaz –imposible como es– no evoca precisamente un escenario idílico, sino más bien una distopía orwelliana, donde cada movimiento puede ser observado, registrado y escudriñado.*

como toma más tiempo, está saliendo retrasado”, explica Eliana Quiroz de Internet Bolivia.

A pesar del incierto futuro político del país, Quiroz cree que el programa difícilmente será abandonado: es un proyecto hecho para la policía, que ha tenido un rol prominente en el proceso del nuevo gobierno transitorio.

Uno de los aspectos más llamativos sobre Bol-110 es que propone un ejercicio de coordinación mayúsculo de instituciones públicas y privadas relacionadas a la atención de urgencias, incidentes, emergencias y desastres, que incluye a la Policía, el sistema de salud, la Defensa Civil y Bomberos. Mediante un mandato de interoperabilidad, estas instituciones están obligadas a compartir información con el programa, por lo que su alcance se expande de manera bastante amplia a lo largo de todo el sistema social.

En ese sentido, Quiroz explica que Bolivia carece de una ley de protección de datos personales que restrinja el modo en que los datos puedan ser utilizados. “La policía depende del Ministerio de Gobierno y el Ministerio tiene, por mandato, la seguridad ciudadana. No hay -que yo sepa- ninguna restricción para utilización de esta tecnología y, me atrevería a decir, que tiene toda la posibilidad, la capacidad y el mandato de hacerlo. El problema es que no tiene el marco legal de protección de datos, porque eso no existe en Bolivia. Tenemos solamente articulado en la Constitución Política del Estado acerca de privacidad, que es muy genérico”.

Esto no es del todo inusual. Aunque la mayoría de los países latinoamericanos en los cuales se ha implementado o existe un proyecto relativo al reconocimiento facial tienen leyes de protección a los datos personales, en la mayoría no existe una mención explícita a los datos biométricos ni su tratamiento, lo cual no necesariamente implica que carezcan de resguardo legal.

Para el caso argentino, Eduardo Ferreyra puntualiza: “La ley no establece expresamente ninguna disposición sobre datos biométricos, pero sí establece una disposición de datos sensibles, y nosotros de ADC creemos que claramente los datos biométricos entran en la definición de datos sensibles, que es información que revele cuestiones básicas de la identidad de una persona. Aparte, el derecho a la privacidad es derecho constitucional argentino y la Corte Suprema y distintos tribunales han dicho que tiene fuerte carácter expansivo, por lo cual, si bien expresamente no lo dice, está claro que pertenece a un dato sensible”.

Una cuestión similar ocurre en Chile, donde los datos sensibles están sujetos al más alto estándar de protección que establece la ley y solamente pueden ser tratados cuando la ley lo autorice, exista consentimiento del titular o sean datos necesarios para la determinación u otorgamiento de beneficios de salud que correspondan a sus titulares. Y aunque no cabe duda de que los datos biométricos califican como datos sensibles,<sup>12</sup> ello no impidió que una cadena de centros comerciales implementara un sistema de reconocimiento facial con fines de seguridad en uno de sus malls a fines de 2018<sup>13</sup> y que anunciara su expansión a otras de sus locaciones en 2019.<sup>14</sup>

La experiencia chilena es particular por una serie de razones. En primer lugar, porque en el caso del sistema de reconocimiento facial de Mall Plaza, se trata de una implementación privada sobre un espacio semi-público. En segundo lugar, porque el software utilizado por la cadena de centros comerciales fue testeado por la Policía de Investigaciones, arrojando una altísima tasa de falsos positivos, que asciende al 90%.<sup>15</sup>

Y en tercer lugar, porque el otro sistema de reconocimiento facial actualmente en funcionamiento no

12 Para mayor información sobre esta interpretación en el caso chileno, ver La biometría en Chile y sus riesgos de Romina Garrido y Sebastián Becker <https://revfono.uchile.cl/index.php/RCHDT/article/view/45825/48403>

13 Más información en <https://www.derechosdigitales.org/12623/sobre-la-ilegalidad-de-la-implementacion-de-un-sistema-de-reconocimiento-facial-en-mall-plaza/>

14 Más información en <https://www.cooperativa.cl/noticias/pais/policial/robos/mall-plaza-implementara-reconocimiento-facial-tras-violentos-asaltos/2019-09-04/081957.html>

15 Más información en <https://derechosdigitales.tumblr.com/post/183543851946/reconocimiento-facial-en-mall-plaza-90-de-falsos>

cumple funciones de seguridad, sino que busca vigilar la administración de un beneficio social. El sistema desplegado en la red de metro de la ciudad de Valparaíso busca controlar que los usuarios de tarjetas de tarifa reducida, estudiantes y personas de la tercera edad, no presten sus tarjetas a otras personas.<sup>16</sup> No hay información respecto a las pérdidas monetarias que esta práctica significa para la red de metro, ni tampoco del costo de la implementación del sistema de reconocimiento facial.

Una cuestión similar ocurre en Brasil. En São Paulo se implementó hace dos años el uso de cámaras de reconocimiento facial en el sistema de transporte público, con la justificación de que ayudarían a evitar el fraude en el uso de beneficios sociales asociados al transporte. En estos dos años el sistema ha bloqueado más de 300 mil tarjetas<sup>17</sup> supuestamente usadas indebidamente. Por otra parte, la municipalidad ha anunciado la suspensión total de las tarjetas anónimas y ha implementado medidas para obligar el registro de las tarjetas con datos de identificación únicos y residenciales. En una ciudad de las dimensiones de São Paulo, el bloqueo o imposibilidad de acceso a medios de transporte puede tener un gran impacto en la vida y el desarrollo de las personas, particularmente aquellas no registradas, como migrantes y las personas sin techo.

Mientras tanto, Argentina ha implementado un proyecto conocido como Sistema de Identidad Digital (SID), con el objetivo de simplificar y agilizar los trámites que realizan las personas con el Estado, permitiendo validar la identidad mediante el uso de reconocimiento facial.<sup>18</sup> Las imágenes son contrastadas con la base de datos del Registro Nacional de las Personas (RENAPER), que contiene las fotografías de todas las personas ciudadanas y residentes en Argentina.<sup>19</sup> ADC mira este desarrollo con bastante preocupación; como explica Eduardo Ferreyra “nos enteramos de casos de gente que no le funcionaba la identificación y no había otra alternativa para verificar identidad. La única respuesta era que prueben de nuevo”. Ante problemas de este tipo, que potencialmente podrían dejara a personas fuera de los programas sociales, producto de fallas en los sistemas de identificación, es necesaria la habilitación de mecanismos alternativos.

*La experiencia internacional ha mostrado que las tecnologías de reconocimiento facial conllevan una serie de problemáticas difíciles de sortear y que las autoridades rara vez mencionan a la hora de anunciar públicamente la intención de poner en funcionamiento un sistema de este tipo.*

Por su parte, en Ecuador avanza una iniciativa del Ministerio de Inclusión Económica y Social, que busca reemplazar el método de registro de poblaciones específicas que usan los servicios del ministerio, particularmente niños, niñas, adolescentes, personas de tercera edad y personas con discapacidades, en condición de pobreza extrema. Por medio de un acuerdo ministerial, el proyecto busca reemplazar el método actual de registro por uno de reconocimiento facial.

“No existe información que de cuenta de cuáles son las deficiencias, las limitaciones y las debilidades del método actual de registro que justifique que sea reemplazado por uno de reconocimiento facial. La información que tenemos es limitadísima”, explica Valeria Betancourt, coordinadora del Programa de políticas de información y comunicación de la

Asociación para el Progreso de las Comunicaciones, APC.

Respecto a los potenciales riesgos, Betancourt es clara: el sistema “Expone a la población más vulnerable a riesgos que son a todas luces desproporcionados. No solo por exacerbar las condiciones de discriminación con base a sesgos que tengan que ver con el color de la piel, prejuicios sociales, sino los riesgos a los que

<sup>16</sup> Más información en <https://derechosdigitales.tumblr.com/post/176557642641/vigilancia-en-el-metro-anuncian-sistema-de>

<sup>17</sup> Más información en <https://agora.folha.uol.com.br/sao-paulo/2019/06/reconhecimento-facial-bloqueia-331-mil-bilhetes-unicos-em-sp.shtml>

<sup>18</sup> Más información en <https://adcdigital.org.ar/portfolio/tu-yo-digital-descubriendo-las-narrativas-sobre-identidad-y-biometria-en-america-latina/>

<sup>19</sup> Más información en <https://adcdigital.org.ar/wp-content/uploads/2019/05/ADC-Fintech-Argentina.pdf>

somete por el uso fraudulento, ilegítimo, político de los datos de estas personas”.

En ese sentido, vale la pena recordar un episodio reciente: en septiembre se conoció la filtración de 18 GB de datos pertenecientes a prácticamente la totalidad de los habitantes de Ecuador,<sup>20</sup> incluyendo números de identificación y de teléfono, registros familiares y de trabajo. Para Betancourt, ese caso de muestra “que no hay capacidad en el sector público para hacer un manejo responsable, eficiente de los datos de los ciudadanos”. Más todavía cuando Ecuador no cuenta con una ley de protección de datos personales que asegure límites basados en el respeto a los derechos fundamentales respecto al uso y aplicación de estos sistemas.

Además del proyecto liderado por el Ministerio de Inclusión Económica y Social, existen actualmente en Ecuador otros dos proyectos que están intentando implementar tecnologías de reconocimiento facial. El primero de ellos busca generar un sistema de videovigilancia orientado a mejorar las condiciones de seguridad de la ciudad de Quito, utilizando a la capital como una experiencia piloto con intenciones de expandirse al resto del país. El segundo, es una iniciativa de la estrategia Ecuador Digital, que está liderada por el Ministerio de Telecomunicaciones y Sociedad de la Información, y que apunta a agilizar los procedimientos alrededor de los trámites en el sector público.

Respecto a las motivaciones detrás de estos proyectos, Betancourt señala que “se piensa que la implementación de estos sistemas de por sí va a resultar un incremento de la eficiencia en los servicios o que de por sí van a mejorar las condiciones de seguridad en los espacios públicos, cuando lo que hemos visto es que si se aplican en las condiciones en las que hemos referido resultaría mucho más problemático que parte de una solución. La implementación de estos sistemas sin una mirada de derechos humanos es terriblemente problemática”.

Esta es solo una muestra del modo en el cual las tecnologías de reconocimiento facial se están implementando por la región. No son los únicos: países como México y Brasil –que utilizó un sistema de reconocimiento facial para vigilar a los participantes de la más reciente edición del Carnaval de Río de Janeiro– están implementando sistemas de este tipo a diferentes escalas y con propósitos diversos, ya sea a nivel de gobierno central o local, e incluso a veces en manos de privados, como en el caso chileno. Y no sería del todo extraño que entre el momento en que se termine de escribir este texto y su posterior publicación, una nueva iniciativa haya sido anunciada en Perú, Panamá o Uruguay.

En el intertanto, la ADC ha introducido una Acción Declarativa de Inconstitucionalidad contra el Gobierno de la Ciudad de Buenos Aires por la resolución que introduce el sistema de reconocimiento facial. TEDIC, junto al Instituto de Derecho y Economía Ambiental (IDEA), presentó una acción de inconstitucionalidad contra las resoluciones que negaron las solicitudes de información sobre el sistema de reconocimiento facial. Por su parte, tanto en Bolivia como en Ecuador se están estudiando los siguientes pasos a seguir en la materia.

## CAPÍTULO 3

# PROBLEMAS DE NUNCA ACABAR

## LAS NUEVAS BATALLAS DEL DERECHO DE AUTOR

Por Jamila Venturini

¿Cuánto ha cambiado internet durante los últimos 20 años en América Latina? A principios de siglo no había redes sociales como las conocemos hoy y el número de celulares presentes en la región todavía era bajo. El uso de la red dependía en gran medida de la disponibilidad de una computadora de escritorio y, a veces, de los horarios más económicos para conectarse desde una línea telefónica. Los contenidos se encontraban distribuidos en una infinitud de portales, páginas web y blogs. Había foros, sitios de chat y aplicaciones de mensajería que era necesario descargar e instalar en la computadora, aunque el principal medio de comunicación era el correo electrónico.

El acceso a la red era mucho más restrictivo de lo que sigue siendo. Según datos de la Comisión Económica para América Latina y el Caribe (CEPAL), en 18 países de la región el porcentaje de hogares con acceso a internet no alcanzaba el 20% en 2005.<sup>1</sup> Chile era el país con la tasa de penetración más elevada, alcanzando el 16,7% de hogares conectados; en 2017, esa cifra alcanzaría el 87,5%. Los números también mejoraron en el resto de la región; entre 2010 y 2016, el total de hogares conectados en 24 países de América Latina y el Caribe subió del 22,4% al 45,5%.<sup>2</sup> Y aunque esta cifra todavía era bastante inferior a las del Norte Global, hay que notar que estos números ocultan grandes desigualdades: la conexión doméstica en países como El Salvador y Nicaragua seguía siendo menor al 20% en 2017.<sup>3</sup>

Siendo este el panorama, en los 2000 los principales debates de activistas en temas digitales giraban en torno al acceso. A las legítimas demandas de mayor y mejor conexión, se sumaba el derecho a descargar, compartir y usar libremente los contenidos disponibles en la red. En ese contexto, los límites a la propiedad intelectual eran una de las disputas centrales en términos de políticas públicas. Y es que las interpretaciones excesivas de las leyes de derechos de autor constituían un peligro real, que amenazaba con restringir acciones banales en el mundo digital, como podría ser un simple copiar y pegar.

Hoy sufrimos intentando entender problemas como el impacto de la desinformación en la democracia, la violencia y el discurso de odio contra los grupos no hegemónicos o la vigilancia gubernamental y privada

1 Ver [https://cepalstat-prod.cepal.org/cepalstat/tabulador/ConsultaIntegradaProc\\_HTML.asp](https://cepalstat-prod.cepal.org/cepalstat/tabulador/ConsultaIntegradaProc_HTML.asp)

2 Ver [https://repositorio.cepal.org/bitstream/handle/11362/43365/1/S1800083\\_es.pdf](https://repositorio.cepal.org/bitstream/handle/11362/43365/1/S1800083_es.pdf)

3 Ver [https://cepalstat-prod.cepal.org/cepalstat/tabulador/ConsultaIntegradaProc\\_HTML.asp](https://cepalstat-prod.cepal.org/cepalstat/tabulador/ConsultaIntegradaProc_HTML.asp)

contra las defensoras de derechos humanos. En ese escenario, las luchas por el acceso al conocimiento y a la cultura parecen ser cosa del pasado. A fin de cuentas, hoy no es necesario eschar blogs especializados o servidores P2P en busca de música y películas. Las plataformas de streaming como Spotify y Netflix se encargan de ello.

Pero, ¿realmente se han vuelto irrelevantes las discusiones sobre derechos de autor? Convendría mirar de cerca los últimos acontecimientos en la región, lo que está ocurriendo en Brasil y Uruguay, que sin levantar mucho polvo confirman que se trata de un tema todavía espinudo y donde la disipación de los esfuerzos puede costar caro. Más todavía, muy lejos de desaparecer, todo pareciera indicar que la problemática se ha complejizado, involucrando perspectivas y consideraciones nuevas, sobre las cuales se hace necesario reflexionar con detenimiento.

### De cómo Europa institucionalizó la censura privada

En materia de derechos de autor, 2019 comenzó con la aprobación de la polémica directiva de la Unión Europea<sup>4</sup> que, entre otras medidas, busca que los proveedores de servicio en línea –como Facebook, Google, Twitter y YouTube– sean judicialmente responsables por las infracciones al derecho de autor cometidas por sus usuarios, a menos que tomen medidas para filtrar o eliminar tales contenidos.

*Las disputas en materia de derechos de autor hoy son mucho más complejas que lo que imaginábamos hace una década y se enmarañan con otras preocupaciones como la privacidad, la libertad de expresión y otros derechos fundamentales. Volver la atención sobre estas discusiones es fundamental.*

La normativa estaba siendo discutida hacía algunos años y fue blanco de duras críticas, incluyendo las del Relator Especial para la Libertad de Expresión de Naciones Unidas, David Kaye, quien afirmó que la propuesta podría incentivar la censura previa al estimular a las plataformas a sobre restringir contenidos legítimos para evitar exponerse a ser sancionadas en caso de que ocurriera una infracción.<sup>5</sup> Activistas de todo el mundo alertaron además de los riesgos para el desarrollo de internet, en tanto la creación de sistemas de detección y eliminación de contenidos es una tarea sumamente compleja y cara de implementar, incrementando la asimetría entre las grandes compañías que cuentan con los recursos para poder cumplir con la normativa y las empresas nuevas y pequeñas.<sup>6</sup>

Sin embargo, las autoridades optaron por ignorarlos y aprobar la medida, respondiendo a las presiones de la industria del derecho de autor y haciendo eco también de un creciente sentimiento antagónico frente a las gigantescas empresas de internet estadouni-

denses y sus repetidos esfuerzos por esquivar la regulación. Pero, si bien el fin puede parecer legítimo, la medida juega a contramano de las más recientes investigaciones –impulsadas con gran fuerza desde América Latina– sobre las graves consecuencias que acarrearán las decisiones algorítmicas tomadas generalmente con gran opacidad y, en muchos casos, por sobre los derechos fundamentales.

Dependiendo de como se implementen los mecanismos exigidos en la directiva y dada la naturaleza global de internet, estas limitantes podrían incluso incidir en el acceso a contenidos desde América Latina<sup>7</sup> y el resto del mundo, contraviniendo las legislaciones locales en materia de derecho de autor y las restricciones

4 Derechos de autor en el mercado único digital. Ver <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P8-TA-2019-0231+0+DOC+XML+V0//ES>

5 <https://www.ohchr.org/Documents/Issues/Opinion/Legislation/OL-OTH-41-2018.pdf>

6 <https://www.derechosdigitales.org/12827/directiva-de-derechos-de-autor-de-la-ue-avanza-la-internet-filtrada-en-europa/>

7 Ver <https://stats.karisma.org.co/la-directiva-europea-de-derecho-de-autor-y-su-impacto-en-los-usuarios-de-america-latina-y-el-caribe-una-perspectiva-desde-las-organizaciones-de-la-sociedad-civil/>

a la responsabilidad de intermediarios vigentes fuera de la Unión Europea. Además, tal como ocurrió con el controvertido derecho al olvido, la aprobación de esta medida en Europa puede legitimar propuestas similares o peores en América Latina, con una clase política muy interesada en restringir las posibilidades de expresión de la ciudadanía.<sup>8</sup>

### Importando las peores ideas

El temor a una ola de propuestas legislativas inspiradas por la directiva europea se justifica cuando tomamos el caso de Brasil, país que ostenta una de las peores normativas en materia de derecho de autor,<sup>9</sup> una que tras menos de 10 años de vigencia fue declarada obsoleta debido a que su carácter restrictivo frenaba muchas de las posibilidades de acceso a la información, conocimiento y cultura potenciadas por las tecnologías digitales.

Hubo intentos a principios de los 2000, con Gilberto Gil a la cabeza del Ministerio de Cultura y gran participación de la comunidad de activistas por la cultura libre, de buscar alternativas más flexibles al modo en que las obras artísticas, científicas y del entretenimiento son distribuidas, experimentadas y usadas.<sup>10</sup> Se impulsó una consulta para reformar completamente la ley, pero, una serie de circunstancias de índole político interrumpieron el esperanzador proceso.<sup>11</sup>

Más de una década después la discusión se ha retomado, aunque con un cariz muy diferente. De forma totalmente inesperada, el gobierno del presidente Jair Bolsonaro abrió a fines de junio una consulta pública<sup>12</sup> sobre la reforma a la ley de derechos de autor. No hubo debate previo, documento preparatorio, mención a los procesos iniciados la década anterior o un texto base que pudiera dar pistas de las intenciones perseguidas. Ante la sospecha que ha generado la consulta, dos elementos llaman la atención: la mención expresa a la directiva europea en el texto que presentaba la consulta y una de las preguntas contenidas en el formulario, sobre la necesidad de realizar una “reforma integral” o limitarla a realizar ajustes acotados a lo relativo a los nuevos modelos de negocios en internet.

Organizaciones de derechos digitales brasileñas llevan años alertando sobre las presiones que la industria del entretenimiento está realizando en favor de mayores restricciones a la circulación de contenidos en línea.<sup>13</sup> Las pistas aportadas por el proceso de consulta hacen sospechar que los cambios que se busca introducir estén alineados con algunas de las propuestas de la directiva europea y deterioren el principio de no responsabilidad de los intermediarios por infracciones de terceros vigente en Brasil. Un cambio de esta naturaleza representaría la victoria de intereses comerciales de la industria por sobre la ciudadanía y el interés público.

Pero si de malas noticias se trata, el premio se lo llevó Uruguay, cuyo parlamento aprobó el 18 de diciembre una extensión de veinte años al plazo de explotación económica exclusiva contemplado en el derecho de autor y los derechos conexos. De esta manera, las obras pasarán a formar parte del dominio público recién 70 años tras la muerte del o la autora.

Se trata de una noticia triste. Uruguay era uno de los pocos países en la región que seguía manteniendo la normativa contemplada en el Convenio de Berna: la vida del autor más 50 años, cuyo carácter de estándar pierde cada vez más peso frente a las sucesivas extensiones que los países han implementado a sus legis-

8 El abuso de las reglas de derecho de autor con el fin de censurar discursos protegidos como la crítica política está bien documentado en la región. Un caso particularmente notorio fue el del gobierno de Rafael Correa en Ecuador. Para más información, ver <https://www.derechosdigitales.org/7955/ecuador-los-derechos-de-autor-como-un-arma-de-censura/>

9 <https://link.estadao.com.br/blogs/tatiana-dias/brasil-tem-a-5a-pior-lei-autoral-do-mundo/>

10 Ver <https://www.nytimes.com/2007/03/11/arts/music/11roht.html>

11 Gil dejó el ministerio en 2008.

12 <http://cultura.gov.br/ministerio-da-cidadania-abre-consulta-publica-sobre-reforma-da-lei-de-direitos-autorais/>

13 <https://feed.itsrio.org/cpi-dos-cibercrimes-equipara-direitos-autorais-a-terrorismo-para-censurar-a-internet-807a17693052?gi=8af199b3df73>

laciones nacionales, negociadas principalmente en el marco de acuerdos de libre comercio con Estados Unidos, y que han sido moldeadas principalmente a la imagen de los deseos de la gran industria del licenciamiento, con empresas como Disney a la cabeza.

Pero no hubo acá ningún acuerdo de libre comercio con nadie. La ley fue aprobada de forma express y prácticamente sin debate previo, justificado en consignas como “Uruguay no puede quedarse rezagado”<sup>14</sup> en una de las materias en que corría con ventaja. Todavía peor: a diferencia de los procesos llevados por Chile, Colombia y México, que modificaron sus legislaciones producto de los acuerdos comerciales, en el caso uruguayo la extensión no vino aparejada de la creación de excepciones en favor de los usuarios de la producción cultural y científica, que compensaran de alguna manera la pérdida del patrimonio común que supone la ampliación del periodo de protección. Y eso no es todo, el proyecto prevé además la compensación retroactiva de los titulares de derecho que dejaron de recibir regalías después de los 50 años.<sup>15</sup>

Así, Uruguay termina el año con una de las peores legislaciones de la región en materia de derechos de autor.

### Las nuevas luchas del derecho de autor

Mucho ha cambiado internet en los últimos años y las luchas que las y los activistas están dando en el plano de lo digital también son diferentes. Pero si la vieja pelea por el acceso a la cultura asociada a los derechos de autor parece un tema superado, no es precisamente porque el problema se haya resuelto, sino más bien que porque la web y el modo de lucrar con ella cambió.

*¿Realmente se han vuelto irrelevantes las discusiones sobre derechos de autor? Convendría mirar de cerca los últimos acontecimientos en la región, lo que está ocurriendo en Brasil y Uruguay, que sin levantar mucho polvo confirman que se trata de un tema todavía espinudo y donde la disipación de los esfuerzos puede costar caro.*

Tras años de insistir en criminalizar a usuarias y usuarios, la industria del licenciamiento buscó sus propios mecanismos para intentar controlar la circulación de obras protegidas, lo que ha devenido en el florecimiento de las plataformas de streaming, con Netflix y Spotify a la cabeza y una serie de competidores cada vez más fuertes intentando quitarles el trono. El éxito de estos servicios puede haber logrado apaciguar los ánimos litigantes de la industria discográfica y las compañías disqueras (o lo que queda de ellas), pero ¿qué hay de nosotras?

Es necesario señalar que el acceso precario que obtenemos al suscribirnos a una plataforma comercial de distribución de música y películas logra evadir elegantemente la riquísima discusión que por más de veinte años se ha dado en torno a los derechos de los usuarios de los bienes culturales en internet y su búsqueda por fortalecer los regímenes de excepciones, para balancear las tendencias maximalistas predominantes en materia de derecho de autor. Y lo hace clausurando el debate técnicamente: en la plataforma solo es posible hacer lo que la plataforma permite, que no es mucho.

No hay que olvidar tampoco que el acceso a estas plataformas acarrea además el almacenamiento de datos de uso y el perfilamiento de nuestros gustos, con todos los riesgos que ello conlleva.

Tampoco hay que olvidar que una de las primeras grandes discusiones públicas en torno a las tomas de decisiones algorítmicas y su impacto negativo en el ejercicio de derechos fundamentales –hoy en boga–

<sup>14</sup> Ver <https://www.elobservador.com.uy/nota/senado-voto-la-extension-de-los-derechos-de-autor-a-70-anos-el-proyecto-paso-a-diputados-201912181400>

<sup>15</sup> Ver <https://www.elobservador.com.uy/nota/senado-voto-la-extension-de-los-derechos-de-autor-a-70-anos-el-proyecto-paso-a-diputados-201912181400>

fue sobre los sistemas de automatizados de protección de derecho de autor, implementado en plataformas como Youtube, su preocupante tendencia a errar en sus juicios y la facilidad con que podía ser explotada con la intención explícita de censurar discursos válidos. Los mismos que impulsa la directiva europea.

Un caso ejemplar de esto es el del Colectivo Intervozes,<sup>16</sup> organización brasileña que lucha por el derecho a la comunicación y que sufrió la remoción de dos videos de su canal en Youtube, donde realizaban una crítica al modo en que mujeres y personas mayores son representadas en televisión, utilizando para ello fragmentos de algunos programas emitidos por Globo y Bandeirantes, dos importantes estaciones televisivas. Y aunque se trata de un uso contemplado y permitido en la ley brasileña de derechos de autor, los videos fueron marcados como infracciones y retirados de la plataforma.

Frente a esta situación, en 2019 Intervozes presentó una demanda<sup>17</sup> al Ministerio Público, para que investigue el proceso de remoción de contenidos de Google, pues según el colectivo, las reglas de Youtube contravienen la Constitución Federal, el Marco Civil de Internet y el Código del Consumidor.

“Youtube ha aplicado criterios para la difusión y mecanismos de remoción de contenidos que comprometen las garantías a la libertad de expresión”, señaló Flávia Lefèvre, abogada y miembro del Consejo Director del Colectivo Intervozes. “Estas reglas son definidas con base en acuerdos comerciales basados en los intereses comerciales de los titulares de derechos de autor sin ningún compromiso con el interés público y abriendo margen para mecanismos subliminales de censura. Es fundamental que esos mecanismos sean verificados de manera amplia por la sociedad. Necesitamos mayor transparencia e información sobre los criterios adoptados y los efectos de su aplicación”, agregó.

El caso de Intervozes no es un incidente aislado. Las disputas en materia de derechos de autor hoy son mucho más complejas que lo que imaginábamos hace una década y se enmarañan con otras preocupaciones como la privacidad, la libertad de expresión y otros derechos fundamentales. Volver la atención sobre estas discusiones es fundamental. Los casos de Brasil y Uruguay son prueba de ello.

---

16 <https://intervozes.org.br/>

17 Ver <https://intervozes.org.br/publicacoes/intervozes-protocola-acao-no-mpf-contra-a-google/>

## CAPÍTULO 4

# ¿DE QUÉ HABLAMOS CUANDO HABLAMOS DE INTELIGENCIA ARTIFICIAL? DECISIONES ALGORÍTMICAS EN AMÉRICA LATINA

Por María Paz Canales

Mientras la brecha entre ricos y pobres se incrementa en el mundo, América Latina sigue siendo la región donde la riqueza se distribuye de forma más desigual. Según la Comisión Económica para América Latina y el Caribe (CEPAL), existen marcados desequilibrios entre los distintos niveles socioeconómicos en aspectos como la esperanza de vida, la mortalidad infantil, la tasa de analfabetismo y el acceso al agua al interior de las viviendas. La altísima inequidad que asola al continente influye directamente en las posibilidades de desarrollo de sus habitantes y en el ejercicio de sus derechos fundamentales.

El impulso que los actores públicos en la región han dado a la implementación de tecnologías automatizadas de toma de decisiones y el desarrollo de IA se funda en la creencia de que estas permitirían solucionar los problemas pertinentes a la función pública más rápidamente o de mejor manera. En Argentina, Chile, Colombia, México y Uruguay se están desarrollando o comienzan a implementarse estrategias nacionales de inteligencia artificial, hojas de ruta que buscan hacerse cargo de las posibilidades y los riesgos que este tipo de tecnologías implica para el contexto local.

Sin embargo, lo primero que es posible constatar es que no existe completo acuerdo respecto de la definición de inteligencia artificial. Hay quien propone que se refiere a la capacidad de una computadora para realizar tareas comúnmente asociadas con seres inteligentes; o a la simulación de procesos de inteligencia humana por parte de máquinas, especialmente sistemas informáticos, incluyendo procesos de aprendizaje, razonamiento y autocorrección; o una tecnología que realiza predicciones sobre la base de la detección automática de patrones de datos.<sup>1</sup>

Pero independientemente de la definición que escojamos, la verdad sea dicha: existe aún bastante camino por avanzar para poder referirnos efectivamente a formas de inteligencia artificial cuando hablamos de las tecnologías que se están realizando e implementando en nuestra región. La mayor parte de los desarrollos

---

<sup>1</sup> Ver <https://medium.com/@chethankumargn/artificial-intelligence-definition-types-examples-technologies-962ea75c7b9b>

tecnológicos que hoy se anuncian son más modestos, abarcando en la mayoría de los casos procesos de automatización en la toma de decisiones o de asistencia a humanos<sup>2</sup> a través de algoritmos que simplifican el procesamiento de grandes volúmenes de información.

Aún así, las implicancias sociales de esta automatización resultan suficientemente relevantes como para prestarles cuidadosa atención. Si nuestros gobiernos prefieren hacerlo bajo el rótulo de la inteligencia artificial, ya sea como consigna aspiracional para marcar su ruta de desarrollo o por simplificación técnica, ello no resulta obstáculo para examinar desde la perspectiva del interés público el impacto de estas tecnologías, que llamaremos genéricamente sistemas automatizados de toma de decisiones o IA.

### ¿Inteligencia artificial para qué?

Todo uso de una herramienta tecnológica es también una expresión de concepciones políticas acerca del grado de agencia, dignidad e igualdad que quiera reconocerse a las personas: las tecnologías impactan de distinta forma a los grupos humanos, de acuerdo a cuestiones como el género, el color de su piel y su clase social, y el modo en que estas características los sitúan socialmente. Por ello, en el marco de un sistema democrático, la adopción de tecnologías exige transparencia a los tomadores de decisiones.

*Los datos recolectados en nuestros países son reflejo fiel de nuestros sistemas políticos, económicos, sociales y culturales. Echar a andar la máquina de la automatización de decisiones implicaría condicionar el futuro a nuestro pasado de discriminación y desigualdad.*

Por lo mismo, la primera pregunta que una comunidad debiera formularse frente a anuncios de implementación de sistemas “inteligentes” es acerca de los objetivos de dicho despliegue tecnológico. Así, lejos de sumergirnos en un tecnosolucionismo de optimismo utópico, deslumbrado por la capacidad de este tipo de tecnologías, las autoridades están en la obligación de abrir un debate democrático con la comunidad respecto de cuáles son los fines que persigue la solución técnica. Y aunque el abanico de opciones puede ser amplio, por lo general pueden ser agrupadas en dos variantes principales: soluciones que buscan abordar problemas de eficiencia y eficacia en el uso de recursos públicos y aquellas que pueden ser utilizadas como componentes para asegurar el ejercicio de derechos y la construcción de justicia social.

Los objetivos anteriores no son en cualquier caso incompatibles, pero son distintos y no siempre se consideran en conjunto en la toma de decisiones públicas sobre la adopción de tecnología. Una aproximación crítica a la implementación de soluciones de IA es esencial para garantizar que sus capacidades para alcanzar el objetivo propuesto puedan ser cuestionadas y, a su vez, poder compararla con otras alternativas existentes respecto a su mayor o menor lesividad del ejercicio de derechos fundamentales cuya protección puede no haberse situado entre los objetivos establecidos. Así se podría determinar, por ejemplo, que el desarrollo tecnológico resulta más perjudicial que benéfico y debe sustituirse por otro tipo de medidas.<sup>3</sup>

En nuestra región la pregunta no debiera ser si nos subimos alegremente al tren del entusiasmo tecnológico y su más reciente novedad, la IA. La pregunta que tanto las autoridades como la ciudadanía debieran intentar responder es para qué, cuándo y en qué proporción estas herramientas tecnológicas constituyen un aporte real al desarrollo con justicia social y cuándo simplemente maquillan o, peor, amplifican la inequidad en la que aún viven sumidas nuestras sociedades.

<sup>2</sup> A la que algunos se refieren como inteligencia humana aumentada.

<sup>3</sup> Ver <https://lpeblog.org/2019/11/25/the-second-wave-of-algorithmic-accountability/>

## Calidad de los datos

La toma automatizada de decisiones y los futuros desarrollos de IA en nuestra región dependen esencialmente de la existencia y disponibilidad de un cúmulo relevante de datos con los cuales los sistemas puedan ser alimentados. El resultado de los procesos de automatización puede ser radicalmente distinto dependiendo de la calidad de los datos provistos.

En América Latina, esto supone un problema: el nuestro es un continente en el cual la discriminación por género, raza, nivel de ingreso, condición social, nivel educacional, edad, opción sexual, entre muchas otras, se encuentra aún tristemente presente en cada decisión cotidiana, del mundo público y privado, e impacta directamente en la libertad y dignidad de sus habitantes. Los datos recolectados en nuestros países son reflejo fiel de nuestros sistemas políticos, económicos, sociales y culturales. Echar a andar la máquina de la automatización de decisiones implicaría condicionar el futuro a nuestro pasado de discriminación y desigualdad. Primero es imperativo realizar un ejercicio real y profundo de cuestionamiento sobre como generar los datos que nos permitan cumplir con los objetivos de justicia social que deberían trazarse para estas herramientas.

En ese sentido, es interesante lo que propone una iniciativa como la Alianza A Plus<sup>4</sup> liderada por Ciudadanía Inteligente y a la que varias organizaciones que trabajan por los derechos digitales en la región nos hemos sumado. Se trata de un esfuerzo que apunta a la necesidad de examinar críticamente los datos desde una perspectiva de género, para asegurar que la implementación de sistemas algorítmicos sea una oportunidad de corrección de la inequidad histórica que enfrentan las mujeres. Necesitamos más iniciativas de este tipo, que miren la calidad de los datos como prerequisite a cualquier desarrollo de cualquier herramienta que honestamente persiga objetivos de justicia social, de modo que no sea otro espejismo de progreso en la región.

### La ética no basta

Sentados los objetivos de interés público para la implementación de sistemas de decisión automatizados y asumiendo un adecuado abordaje de la calidad de los datos utilizados para no traicionar dichos objetivos, queda analizar el modo de implementar tales sistemas desde la perspectiva del impacto en los derechos de los ciudadanos a los cuales se propone servir.

Expertos de múltiples disciplinas en la región<sup>5</sup> y fuera de ella<sup>6</sup> claman por un tratamiento ético de los datos en IA, como forma de enfrentar los riesgos que su implementación puede tener en la afectación de derechos. Sin embargo, quienes trabajamos en la vereda de la promoción y protección de derechos fundamentales creemos que la ética es un punto de partida que no agota ni satisface las exigencias normativas ya vigentes, como es el marco internacional de los derechos humanos, así como las garantías constitucionales que cada país provee a sus habitantes.

La protección específica de tales derechos clama por regulaciones que puedan asegurar su efectividad en el presente y también en el futuro, cuando el ejercicio de estos derechos dependerá crecientemente de sistemas inescrutables que determinarán el acceso a programas de protección social,<sup>7</sup> la resolución de conflictos judiciales<sup>8</sup> o la libertad de personas enjuiciadas criminalmente.<sup>9</sup> Lo que todas esas iniciativas tienen en común es que son mecanismos de control sobre personas en situación de vulnerabilidad, expuestas a intervenciones que no tienen capacidad de consentir. Imponer sistemas opacos cuyas decisiones limitan

4 <https://aplusalliance.org/>

5 Ver <https://publications.iadb.org/es/la-gestion-etica-de-los-datos>

6 <https://www.oecd.org/going-digital/ai/principles/>

7 Alerta Niñez en Chile. <http://www.crececontigo.gob.cl/wp-content/uploads/2019/12/OOTT-OLN.pdf>

8 Como Prometea en Argentina [https://ialab.com.ar/wp-content/uploads/2019/05/prometea\\_oea-1.pdf](https://ialab.com.ar/wp-content/uploads/2019/05/prometea_oea-1.pdf)

9 Como Prisma en Colombia. <https://www.elespectador.com/noticias/judicial/prisma-el-programa-de-la-fiscalia-para-predecir-la-reincidencia-criminal-articulo-867214>

los derechos de las personas, sin otorgarles a las afectadas ningún margen de autonomía respecto a su participación, ni la posibilidad de apelar, reclamar y -eventualmente- exigir reparaciones, refuerza y amplifica las injusticias que originalmente produjeron las situaciones de vulnerabilidad.

La ética no basta, en los estados democráticos en los que existe un compromiso normativo de promoción y protección de los derechos humanos, aquellas tecnologías que impactan de manera fundamental el ejercicio de derechos civiles, políticos, económicos, sociales y culturales, reclama intervención regulatoria, cualquiera sea la forma creativa, multidisciplinaria y flexible con la cual los Estados puedan aproximarse a dicho desafío. La innovación, lejos de verse perjudicada, podrá desarrollarse en un marco sostenible y provista de los incentivos económicos adecuados para un desarrollo humano integral.

### Derechos implicados más allá de la privacidad

¿No es suficiente con ocuparnos de la protección de los datos personales para resolver los riesgos de la automatización para el ejercicio de derechos de las personas? Más de una vez nos ha tocado hacer frente a esta pregunta, formulada por gobiernos, la comunidad técnica, organizaciones internacionales para el desarrollo, académicos, legisladores, prensa y un largo etcétera. Y la respuesta es no. La regulación de datos personales es sin duda una pieza esencial para la adecuada operación de la IA, pero no la única.

*La ética no basta, en los estados democráticos en los que existe un compromiso normativo de promoción y protección de los derechos humanos, aquellas tecnologías que impactan de manera fundamental el ejercicio de derechos civiles, políticos, económicos, sociales y culturales, reclama intervención regulatoria, cualquiera sea la forma creativa, multidisciplinaria y flexible con la cual los Estados puedan aproximarse a dicho desafío.*

En nuestra región, Bolivia y Ecuador carecen totalmente de marcos legales de protección de datos personales; Brasil y Paraguay carecen de autoridades independientes para asegurar el adecuado cumplimiento de la normativa existente; las limitaciones en sus competencias le impiden a la autoridad colombiana supervisar adecuadamente a los organismos públicos y a la autoridad chilena fiscalizar a los privados. Ni hablar del nivel de actualización de los estándares imperantes en la región: cuestiones como el tratamiento automatizado de grandes volúmenes de datos, transparencia y explicabilidad algorítmica, obligaciones de intervención humana, auditoría algorítmica, entre otros conceptos, no son abordados por las legislaciones locales.

Todo esto para decir que los estatutos normativos de protección de datos personales no resultan aptos para proveer un marco de control y supervisión a la implementación de AI en nuestra región.

Ahora, de vuelta al punto central, si bien un gran número de riesgos implicados en la implementación de sistemas automatizados de toma de decisiones puede abordarse desde el ángulo de los datos personales, por las implicancias indivi-

duales que ellas traen, muchos de estos riesgos se materializan en la limitación del ejercicio de derechos colectivos, de naturaleza económica, social o cultural, que impactan no a uno sino a grupos completos de individuos que pueden resultar masivamente discriminados, vigilados y censurados por estas tecnologías.<sup>10</sup>

Tal como lo desarrolla el *Global Information Society Watch 2019*,<sup>11</sup> publicado por la Asociación para el Progreso de las Comunicaciones (APC), diferentes formas de inteligencia artificial o toma de decisiones automa-

<sup>10</sup> Ver Monique Mann y Tobias Matzner, Challenging algorithmic profiling: The limits of data protection and anti-discrimination in responding to emergent discrimination.

<sup>11</sup> Disponible en [https://giswatch.org/sites/default/files/gisw2019\\_artificial\\_intelligence.pdf](https://giswatch.org/sites/default/files/gisw2019_artificial_intelligence.pdf)

tizadas abarcan la provisión de servicios básicos “desde el transporte hasta la salud; desde la agricultura hasta la eliminación de desechos; desde la vigilancia hasta el bienestar, y desde la tecnología inteligente en el hogar hasta la exploración espacial. La toma de decisiones automatizada se usa cada vez más en servicios críticos y en la provisión de infraestructura en áreas como el empleo, la vivienda, el acceso a la educación, el comercio y el acceso al crédito, lo que impacta la vida de las personas de manera profunda”. La implementación de este tipo de tecnologías es una forma de modelamiento del comportamiento no solo individual, sino de interacciones sociales y económicas completas, que pretenden ser redibujadas a través de ellas.

Por último, cabe preguntarse por el rol que a estas tecnologías pueden haber para promover el cumplimiento de los Objetivos de Desarrollo Sostenible (ODS) de las Naciones Unidas,<sup>12</sup> que exigen que las iniciativas para acabar con la pobreza a través del crecimiento económico aborden de forma prioritaria una serie de necesidades sociales como la educación, la salud, la protección social y las oportunidades de empleo, a la vez que promueven la protección del medio ambiente, la promoción de equidad de género e inclusión y la reducción de la desigualdad.

Desde el marco que proveen los estándares internacionales de derechos humanos, las regulaciones que se desarrollen en torno a los sistemas automatizados de toma de decisiones deberían apuntar a salvaguardar la dignidad humana, asegurar la agencia colectiva e individual, y a materializar la equidad y la justicia social. En todo ello la privacidad es un componente esencial que requiere de actualización urgente, pero no agota como herramienta los ámbitos de riesgos generados por estas tecnologías.

### ¿Cómo se están desarrollando las estrategias de inteligencia en nuestra región?

A partir de su Política de Gobierno Digital,<sup>13</sup> Uruguay fue pionero en la región en desarrollar una Estrategia de Inteligencia Artificial para el Gobierno Digital.<sup>14</sup> Ambos documentos se basan en el principio de transformación digital con equidad. Y es precisamente con ese principio inspirador que el proceso se condujo con gran apertura, consultando a los diferentes sectores sociales, incluyendo empresas de distintos tamaños, la academia, la comunidad técnica y la sociedad civil. Se aplicaron los principios de cocreación y participación ciudadana previamente establecidos en el Plan de Acción Nacional de Gobierno Abierto, convocando un proceso de consulta pública en cuatro etapas<sup>15</sup> entre abril y junio de 2019.<sup>16</sup> En la actualidad, Uruguay se encuentra en la fase de elaboración de guías y manuales de buenas prácticas en el marco de la estrategia de inteligencia artificial definida.

En los otros países de la región que se han embarcado en el diseño de estrategias de inteligencia artificial, el proceso ha sido más opaco y poco abundante de mecanismos efectivos de participación que puedan orientarlas hacia el debate multisectorial, multidisciplinario e inclusivo que requieren.

En agosto de 2018, Argentina presentó la hoja de ruta para el diseño del Plan Nacional de Inteligencia Artificial,<sup>17</sup> que contemplaba la convocatoria de diversos sectores para participar de mesas de trabajo por eje

12 <https://www.un.org/sustainabledevelopment/es/sustainable-development-goals/>

13 [https://uruguaydigital.gub.uy/wps/wcm/connect/urudigital/6bd54ea6-1207-4cfa-bafb-c859bdac8019/Descargar+Agenda+Digital+2020+%2Bactualizacion+de+medio+termino%29.pdf?MOD=AJPERES&CONVERT\\_TO=url&CACHEID=6bd54ea6-1207-4cfa-bafb-c859bdac8019](https://uruguaydigital.gub.uy/wps/wcm/connect/urudigital/6bd54ea6-1207-4cfa-bafb-c859bdac8019/Descargar+Agenda+Digital+2020+%2Bactualizacion+de+medio+termino%29.pdf?MOD=AJPERES&CONVERT_TO=url&CACHEID=6bd54ea6-1207-4cfa-bafb-c859bdac8019)

14 <https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/sites/agencia-gobierno-electronico-sociedad-informacion-conocimiento/files/documentos/publicaciones/Estrategia%20IA%20-%20versi%C3%B3n%20espa%C3%B1ol.pdf>

15 Las etapas fueron las siguientes:

Etapa I: Consulta sobre principios generales que deben guiar la aplicación de Inteligencia Artificial en el Estado.

Etapa II: Sistematización y análisis de propuestas

Etapa III: Consulta sobre la Estrategia de Inteligencia Artificial y

Etapa IV: Aprobación del Documento final de Estrategia de Inteligencia Artificial

16 <https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/comunicacion/noticias/consulta-publica-inteligencia-artificial-para-el-gobierno-digital?idPadre=1937>

17 <https://www.uai.edu.ar/ciiti/2019/buenos-aires/downloads/B1/JA-Plan-Nacional-IA.pdf>

estratégico y alguna instancia virtual de elaboración de recomendaciones por eje, dando paso luego a un trabajo conjunto sobre documentos de recomendaciones, líneas de acción propuestas y objetivos, todo ello en un calendario hasta junio de 2019. Durante este tiempo solo se han realizado varias conferencias que buscan desarrollar conversaciones a nivel local en la materia, con predominante participación del sector privado y la academia.

Durante el mes de agosto de 2019 en Chile, el ministro de Ciencia, Tecnología, Conocimiento e Innovación convocó un comité de diez expertos para apoyar la elaboración de la Política Nacional de Inteligencia Artificial que el gobierno pretende presentar en abril 2020. De este comité de expertos se espera un diagnóstico de la situación del país en IA y propuestas en tres áreas de trabajo: factores habilitantes; desarrollo y adopción de IA y un último ámbito vinculado a ética, estándares, seguridad y regulación del uso de estas tecnologías.<sup>18</sup> Los expertos seleccionados, de alto nivel académico y trabajo internacional en su mayoría, no son representativos de una discusión inclusiva de la sociedad chilena y no existe a la fecha transparencia acerca de cómo se desarrollarán sus actividades para incorporar el aporte en el trabajo del comité de distintos sectores.

En Colombia, el desarrollo de una política de transformación digital terminó súbitamente en convertirse también en una estrategia de IA. El documento aprobado en noviembre de 2019 contiene principios tales como la creación de un mercado de IA en el país, la atracción de talento internacional y la cooperación internacional.<sup>19</sup> La política se desarrolló en el marco del proceso “*Going Digital*” impulsado por la OECD, pero las instancias de consulta desarrolladas, con participación del sector privado, la sociedad civil y comentarios de instituciones internacionales, apuntaron primariamente a los aspectos de transformación digital -centro de la política en su origen- y no necesariamente a los aspectos relacionados con IA que fueron agregados con posterioridad.

En México, en marzo de 2018, se anunciaba un mapa de ruta para una estrategia de IA en el país.<sup>20</sup> Con posterioridad, y con un plazo brevísimo de duración que iba del 15 de agosto al 15 de septiembre de 2108, se desarrolló una encuesta nacional.<sup>21</sup> La encuesta contó con 1585 participantes, 62% de hombres y 37% de mujeres, con 50% de los participantes localizados en el Estado de México. La participación del sector social fue del 3%, mientras que la de gobierno, iniciativa privada y academia representó el 92%. Si bien la encuesta se posicionó como un intento de “democratizar la conversación sobre IA, despertar el interés de nuevos sectores en el tema y recoger los puntos de vista de la ciudadanía con relación a la percepción del impacto de las nuevas tecnologías en su vida cotidiana”, la breve extensión de su plazo, así como la participación en la misma, no dan cuenta de un verdadero debate inclusivo de amplios sectores de la sociedad.

Desde nuestra perspectiva, y tomando en consideración la experiencia regional desarrollada en la construcción de Estrategias Nacionales de Ciberseguridad,<sup>22</sup> resulta esencial asegurar proceso amplios de participación de múltiples partes interesadas con conocimientos en diversas disciplinas que representen un espectro inclusivo de nuestras sociedades. Esta modalidad permite incorporar distintas visiones y aproximaciones, así como recoger todos los antecedentes necesarios para que dichas políticas sean elaboradas en base a la evidencia. La participación multisectorial no solo vuelve los procesos más abiertos, transparentes y democráticos, sino que tiene el potencial de mejorar la calidad de los mismos, especialmente en temas sistémicos y que involucran diversos factores, como es el caso de las estrategias de IA.

## Desde los estándares a lo práctico

Las estrategias y los estándares son sin duda importantes a la hora de trazar las grandes líneas que deben inspirar las políticas públicas. A las estrategias en desarrollo y sus falencias ya nos hemos referido. En

18 <https://www.gob.cl/noticias/ministerio-de-ciencia-presenta-comite-asesor-del-gobierno-en-inteligencia-artificial/>

19 [https://www.mintic.gov.co/portal/604/articles-107147\\_recurso\\_1.pdf](https://www.mintic.gov.co/portal/604/articles-107147_recurso_1.pdf)

20 <https://www.gob.mx/mexicodigital/articulos/estrategia-de-inteligencia-artificial-mx-2018>

21 [https://36dc704c-0d61-4da0-87fa-917581cbce16.filesusr.com/ugd/7be025\\_9e91bffffeea647a0a663630ea716aa8f.pdf](https://36dc704c-0d61-4da0-87fa-917581cbce16.filesusr.com/ugd/7be025_9e91bffffeea647a0a663630ea716aa8f.pdf)

22 <https://www.derechosdigitales.org/wp-content/uploads/ciberseguridad.pdf>

cuanto a los estándares, si bien a la fecha no existe un conjunto de tipificaciones que hayan sido desarrolladas particularmente para la región, alrededor del mundo - y fruto del esfuerzo de entidades nacionales, públicas, privadas, académicas e internacionales - se cuentan más de 80 cuerpos de principios, guías o estándares técnicos referidos a IA, conforme es reportado por investigadores internacionales.<sup>23</sup> A ellos se suma el reciente anuncio de UNESCO, que busca desarrollar un set de principios que represente la visión de Naciones Unidas en la materia, y para lo cual se encontrará realizando una serie de consultas que inició con una reunión en São Paulo, en la cual una comunidad de expertos de América Latina se dio cita este diciembre.

Frente a la proliferación de estándares cabe preguntarse si vale la pena alocar esfuerzo adicional en el desarrollo de más cuerpos de principios, o si aquellos ya desarrollados, iluminados por una interpretación progresiva del marco internacional de derechos humanos son una guía suficiente. Desde nuestra región puede existir una relevante oportunidad de enfocarnos en una aproximación más práctica de la materia, aprovechando todo lo ya debatido y las tendencias comunes en los principios identificados que hablan de

transparencia, justicia y equidad, no maleficencia, responsabilidad y privacidad, que se repiten a través de distintos estándares, aunque con divergencia en su interpretación.<sup>24</sup>

*Lejos de sumergirnos en un tecnosolucionismo de optimismo utópico, deslumbrado por la capacidad de este tipo de tecnologías, las autoridades están en la obligación de abrir un debate democrático con la comunidad respecto de cuáles son los fines que persigue la solución técnica.*

Desde Derechos Digitales proponemos un enfoque centrado en el desarrollo de sistemas de evaluación de impacto en el ejercicio de derechos de las tecnologías automatización de toma de decisiones e IA, tanto desde la perspectiva de los tomadores de decisiones públicos como privados, así como por las agencias de cooperación internacional que en muchos casos financian el desarrollo de tales tecnologías en la región.

Como organización, en este esfuerzo nos hemos vinculado con iniciativas tales como el B-Tech Project,<sup>25</sup> conducido por la Oficina de la Alta Comisionada de Derechos Humanos de las Naciones Unidas, el cual busca mejorar la calidad de implementación de los Principios Rectores de Naciones Unidas

sobre Empresas y Derechos Humanos con respecto a industrias de tecnología. Si bien el trabajo se encuentra aún en desarrollo, este se beneficiaría de una mayor participación de representantes de América Latina, que aporten nuestras visiones de cómo las industrias de toma de decisión automatizada y su vínculo con los estados está impactando el ejercicio de derechos en nuestra región.

En este mismo sentido, una iniciativa que merece particular atención es la alianza fAIr LAC, liderada por el Banco Interamericano de Desarrollo, que reúne representantes de sector público, privado y sociedad civil para asegurar la adopción responsable y generalizada de IA en América Latina y el Caribe.<sup>26</sup> La iniciativa pone énfasis en “aprovechar los beneficios de una inteligencia artificial confiable, que pone al ciudadano en el centro de las decisiones, a la vez que identifica sus desafíos éticos y de privacidad, y tiene mecanismos para mitigarlos”. Aunque el enfoque en el tratamiento ético de los datos y las consideraciones de privacidad se queda corta por las razones antes señaladas, tiene un enorme potencial en la creación de pautas concretas de evaluación del diseño, implementación y seguimiento de proyectos para apoyar el trabajo de los gobiernos en la implementación de sistemas automatizados de toma de decisiones e IA centradas en la inclusión y la justicia social.

23 Ver Jobin, A., Ienca, M. & Vayena, E. The global landscape of AI ethics guidelines. *Nat Mach Intell* 1, 389–399 (2019) doi: 10.1038/s42256-019-0088-2, <https://www.nature.com/articles/s42256-019-0088-2>

24 Jobin, A., Ienca, M. & Vayena, E. Op. Cit.

25 <https://www.ohchr.org/EN/Issues/Business/Pages/B-TechProject.aspx>

26 <https://www.iadb.org/es/fairlac>

Las decisiones automatizadas afectan de manera diferencial a los grupos más vulnerables, si ello no es visibilizado y expresamente combatido desde los objetivos de la implementación de dichas tecnologías, se conduce a reforzar procesos de control social y precarización que han estado en la base de la construcción de muchas de nuestras sociedades, tanto para asegurar la dominancia de las clases sociales y económicas más privilegiadas, como para facilitar la explotación de los más vulnerables.

Si bien el marco internacional de los derechos humanos no es por sí suficiente para hacer frente a cuestiones de justicia social, aún constituye una herramienta capaz de controlar las implementaciones tecnológicas que sirvan al desarrollo humano con agencia y dignidad, en la medida en que se releven tanto las dimensiones colectivas de los derechos humanos y no solo las individuales, así como el valor de los derechos económicos, sociales, culturales y ambientales como parte de un sistema único e interconectado de derechos de igual valor para la realización de una democracia con justicia social en nuestra región.

La promesa de la tecnología es la mejora de nuestras vidas y ella puede ser de tremendo valor para nuestra región. Liberar ese valor para la inclusión y la justicia social depende de poner esos objetivos como centrales en la hoja de ruta y no usar limitados sustitutos como el tratamiento ético de los datos. Los desarrollos y despliegues tecnológicos no deberían resultar en nuevas formas de discriminación, que con la eficiencia o la eficacia como bandera profundicen otras desigualdades como daño colateral que debemos asumir en favor de un supuesto bien mayor representado por el progreso.

Un debate democrático inclusivo de la implementación de tecnologías y una aproximación práctica a los derechos fundamentales desde la creación de sistemas de evaluación de impacto en el diseño, implementación y seguimiento de proyectos de IA es la forma más concreta de poner estas tecnologías al servicio del cierre de las brechas de desigualdad e inclusión en el desarrollo en que aún vive nuestra región.

## CAPÍTULO 5

# LA CRIMINALIZACIÓN DEL CONOCIMIENTO TÉCNICO LA PERSECUCIÓN DE ACTIVISTAS DIGITALES EN AMÉRICA LATINA

Por Vladimir Garay

“Las organizaciones de la sociedad civil firmantes expresamos nuestra preocupación por la tendencia mundial de perseguir a las personas que defienden los derechos humanos utilizando medios y plataformas digitales, incluidas quienes realizan investigaciones y proveen entrenamientos de seguridad para proteger y promover estos derechos”.<sup>1</sup> Así comienza una declaración firmada por numerosas organizaciones promotoras de los derechos fundamentales en los entornos digitales y coordinada en el marco del Foro de Gobernanza de Internet realizado en Berlín en noviembre de 2019.

La declaración expresa su rechazo a los distintos casos de activistas que están siendo perseguidos, judicial y políticamente, por el ejercicio de su trabajo técnico, demandando reconocimiento del valor de sus contribuciones a nivel legal, social y político. Algunos nombres de alto perfil son mencionados a modo de ejemplo: Alaa Abd El Fattah,<sup>2</sup> blogger, desarrollador de software y activista político en Egipto; el escritor y académico Fikret Baskaya<sup>3</sup> en Turquía o Ahmed Mansoor,<sup>4</sup> disidente político emiratí, acusado y encarcelado por mantener un sitio web que expresaba visiones contrarias al gobierno.

Particularmente grave es la inclusión de dos casos controvertidos casos latinoamericanos: la detención del activista sueco Ola Bini, ocurrida en Ecuador en abril de 2019 y la investigación de Javier Smaldone en Argentina, acusado de participar en el robo y difusión de información policial sensible. En ambos casos se trata de expertos informáticos que están enfrentando procesos judiciales donde las pruebas de su participación en actividades ilícitas son escasas y el proceder cuestionable, parte de una “tendencia mundial creciente y peligrosa”.<sup>5</sup>

1 Ver <https://www.derechosdigitales.org/14065/declaracion-para-la-proteccion-de-los-defensores-de-los-derechos-digitales/>

2 [https://en.wikipedia.org/wiki/Alaa\\_Abd\\_El-Fattah](https://en.wikipedia.org/wiki/Alaa_Abd_El-Fattah)

3 <https://ifex.org/terrorist-propaganda-charges-against-fikret-baskaya-must-be-dismissed/>

4 [https://en.wikipedia.org/wiki/Ahmed\\_Mansoor](https://en.wikipedia.org/wiki/Ahmed_Mansoor)

5 Ídem

Javier Smaldone es un viejo conocido de las autoridades argentinas. Informático, desarrollador de software libre y experto en seguridad, Smaldone fue uno de los más fervientes críticos del sistema de voto electrónico y de la empresa Smartmatic, ya sea en el plenario de comisiones sobre la reforma electoral de 2016, donde demostró en el Congreso las falencias del sistema<sup>6</sup> o en su cuenta de Twitter, red social de la que es un usuario asiduo y notorio, con casi 25 mil seguidores. Y, de cierta forma, esta historia comienza con un RT.

El 12 agosto de 2019 la cuenta de Twitter @lagorraleak comenzó a difundir información sustraída de la Policía Federal Argentina y de la Policía de la Ciudad de Buenos Aires. Más de 700 GB de datos que, entre otras cosas, contenían copias de escuchas telefónicas, documentos administrativos y -lo más grave- información sensible del personal de la Superintendencia de Drogas Peligrosas: teléfonos personales, direcciones y nombres de parejas, hijas e hijos de alrededor de 70 policías fueron distribuidos a través de internet.<sup>7</sup>

*La “des-elitización” del ámbito digital y el constante acercamiento de las organizaciones que se dedican a esto con otro tipo de organizaciones -movimientos de mujeres, de género, sindicatos y demás organizaciones que tienen una lógica contestaria frente a algunas relaciones de poder- se vuelve una necesidad.*

La información circuló ampliamente y Smaldone fue uno de los tantos que comentó lo que había pasado. “Solo con esos antecedentes, con capturas de pantalla de sus conversaciones de Twitter y documentación de sus conocimientos de informática, la Policía Federal lo sindicó como sospechoso y lograron que un juez les autorizara un allanamiento de su domicilio” -explica Beatriz Busaniche, presidenta de Fundación Vía Libre, una de las principales organizaciones aliadas de Smaldone en este embrollo- “se ese allanamiento se llevaron todos sus equipos informáticos y se lo llevaron esposado. Lo tuvieron privado de su libertad durante varias horas sin hacerle ninguna imputación concreta; al día de hoy no hay una imputación, no se sabe de qué se lo acusa”.

Javier Smaldone lo calificó como una persecución política. “me detuvieron por informar” declaró Javier Smaldone en una entrevista radial.<sup>8</sup> Al obtener acceso a la carpeta investigativa, el experto informático y su círculo pudo comprobar, no sin cierta sorpresa, la escala de la investigación: “Pusieron

todo el aparato de vigilancia del estado para monitorear sus actividades. Mandaron poner cámaras de vigilancia en el domicilio de los hijos de Javier; pidieron toda la documentación de la tarjeta de transporte de Javier y de su pareja. Tomaron fotografías de Javier y de su pareja en lugares públicos. Pidieron una interceptación de su teléfono y, además, volcaron a la prensa que él estaba sindicado como el autor de las filtraciones sobre la policía federal”, explica Busaniche.

Para la presidenta de Fundación Vía Libre, el caso es doblemente grave, pues no solamente expone la persecución de la que pueden ser víctimas las voces críticas en Argentina, sino que además desnuda las negligentes condiciones con las que la Policía trata información sensible. Y es que la filtración de agosto no es la primera: en 2017 La Policía Federal argentina fue víctima de un ataque similar y se sospecha que ambos casos son atribuibles a la(s) misma(s) persona(s), cuya identidad sigue siendo un misterio. “Es doblemente irresponsable, no solo por cómo están jodiéndole la vida a Javier, a su pareja y a su familia, sino también porque no están investigando un hecho grave, que es la filtración de información sensible de las fuerzas de seguridad”, manifiesta Busaniche.

6 Ver <https://www.pagina12.com.ar/224209-el-arresto-de-javier-smaldone-critico-de-smartmatic-y-el-vot>

7 Ver <https://www.infobae.com/sociedad/policiales/2019/08/16/la-gorra-leaks-que-hay-en-los-archivos-secretos-de-la-policia-filtrados-por-hackers/>

8 Ver [https://www.nexofin.com/notas/839085-javier-smaldone-rompio-el-silencio-y-revelo-por-que-la-justicia-ordeno-su-detencion-n-/](https://www.nexofin.com/notas/839085-javier-smaldone-rompio-el-silencio-y-revelo-por-que-la-justicia-ordeno-su-detencion-n/)

La rigurosidad de la investigación y el poco apego a los protocolos establecidos por el debido proceso son algunos de los puntos más críticos del caso. Más todavía cuando no parece haber ninguna pista certera respecto a los atacantes y las pruebas contra Smaldone carecen de base sólida; como explica Busaniche: “es muy interesante ver que hacen inteligencia de fuente abierta: opiniones volcadas en Twitter; ‘animadversión a la policía manifiesta’ a raíz de sus tuits; bromas, que tendrían supuesto valor probatorio. Y otro de los argumentos es que tiene los conocimientos de informática necesarios como para hacer una operación de este tipo. Es decir, todo lo que tienen en su contra es sus conocimientos de informática y sus opiniones en Twitter”.

### Ecuador: Ola Bini

En una entrevista concedida a CNN en Español, enmarcada en su participación en la Asamblea General de Naciones Unidas, el presidente ecuatoriano, Lenín Moreno, declaró que el señor Ola Bini “ha intervenido no solamente en la política del Ecuador, sino del mundo entero”.<sup>9</sup> Se trata de una acusación grave, que le costó a Bini más de dos meses de prisión preventiva, pero que –al igual que en el caso de Javier Smaldone en Argentina– parece carecer de sustento. “¿Cómo se interviene en la política de todo el mundo? No tiene sentido”, ironiza con amargura Rodrigo Adriel, quien ha ocupado un rol importante en la coordinación de los esfuerzos en apoyo al informático sueco.

Programador y reconocido activista por los derechos fundamentales en los entornos digitales -con un destacado curriculum que incluye participaciones en el desarrollo de proyectos como Enigmail, Letsencrypt y Tor, entre otros-<sup>10</sup> Ola Bini está radicado en Ecuador desde 2013. El 11 de abril de 2019, algunas horas después de que el Gobierno del Ecuador anunciara el retiro del asilo político a Julian Assange en su embajada en Londres, Bini es detenido en el aeropuerto de Quito, mientras esperaba abordar un vuelo a Japón.

“En principio no queda muy claro por qué, pero la entonces Ministra de Interior, María Paula Romo, anuncia que en el contexto del retiro del asilo también estaban buscando en Ecuador a algunos colaboradores de Wikileaks y de Julian Assange, entre los que se encontraban agentes rusos”. explica Adriel. Ahora queda claro que se refería a Bini, quien nació en Gotemburgo, Suecia. “Primero dicen que es un ruso; la orden de detención, que llega después de detenerlo, decía que era suizo y es sueco. Así que mayor idea de lo que estaban haciendo no tenían”, acota Adriel.

En su momento, la Ministra Romo –que hoy ostenta el cargo de Ministra de Gobierno– justificó la detención explicando que el Gobierno quería prevenir que Ecuador se convierta en un centro de “espionaje y piratería” digital<sup>11</sup> y que, aunque no podía comentar la evidencia en contra de Bini, el informático había visitado a Julian Assange al menos “una docena de veces”.<sup>12</sup> “Culpable por asociación” titulaba José María León en la edición latinoamericana del New York Times. Y es que más allá de su vinculación con el director de Wikileaks, el resto de la evidencia parece carecer de sustento”.

“Evidentemente Ola es amigo de Julian Assange. Eso, como sabemos, no constituye delito. Pero por haberlo visitado en la embajada, vestirse raro y tener muchos libros en inglés sobre encriptación, y tener muchos USB y muchas computadoras, era sospechoso y encarcelarlo servía para justificar, en el plano nacional, una decisión del plano geopolítico que es el retiro del asilo a Assange”, explica Adriel.

A pesar de la debilidad de las pruebas, Ola Bini tuvo que pasar 70 días en prisión hasta que, en el mes de julio y tras varios intentos de su defensa, el juzgado de la Corte de la provincia de Pichincha decide otorgarle el habeas corpus y ordena su inmediata liberación, aduciendo un sinnúmero de violaciones y vulneraciones al debido proceso en el marco de su detención.

9 Ver <https://cnnespanol.cnn.com/2019/09/26/lenin-moreno-correa-debe-regresar-y-responder-a-las-acusaciones-en-su-contra/>

10 Ver <https://freeolabini.org/es/about-ola/>

11 <https://www.nytimes.com/es/2019/04/21/ecuador-bini-wikileaks-assange>

12 Idem

Con Ola Bini en libertad, el caso entró en una nueva fase de características kafkianas, que lo mantienen actualmente sin fecha para la audiencia preparatoria de juicio, postergada tras el estallido social ocurrido en el mes de octubre, y -peor todavía- sin juez a cargo.

“Frente a las irregularidades del caso, la defensa pidió la recusación de la jueza Yadira Proaño. Desde el momento en el que Yadira Proaño está recusada no puede seguir conociendo el caso, de tal manera que se tenía que sortear un nuevo juez. Sin embargo, por un error, se sortean dos juezas -explica Adriel. Después de eso ambas juezas empezaron a enviarse comunicaciones argumentando que no tenían competencia para conocer el caso y que le correspondía a la otra. O sea, ninguna de las dos juezas sorteadas se quiere hacer cargo del proceso”.

*El problema es todavía más complejo en tanto las mismas plataformas que permiten circular, amplificar y compartir información relevante para la discusión y la organización de la protesta política, en sus diferentes formas, puede ser también utilizada por el poder estatal para la persecución y la criminalización de quienes participan en ella.*

Así las cosas, hoy Ola Bini y su defensa mantienen la convicción de que la causa debe ser archivada: “no puede haber juicio, básicamente porque no hay prueba de ningún delito y porque no hay delito. Eso es lo que tiene que pasar”, plantea Rodrigo Adriel.

#### Activistas, hackers y delincuentes

Tanto Rodrigo Adriel como Beatriz Busaniche consideran que los casos de Javier Smaldone y Ola Bini ejemplifican una tendencia peligrosa a criminalizar el conocimiento informático. “Hay una desconfianza construida alrededor de la figura de las personas que trabajan en seguridad informática, se ha construido un imaginario sobre ellos que es muy serio, se los deja siempre parados ahí muy en la cercanía de la delincuencia”, explica la presidenta de Fundación Vía Libre. Para Busaniche se vuelve sumamente necesario centrar la atención en las agendas de ciberseguridad, donde se juegan gran parte de los “los intentos por criminalizar el conocimiento informático, que han permeado lentamente en las legislaciones penales de nuestros países”.

“Creo que esto no reconoce izquierda ni derecha, no reconoce demasiada línea ideológica, me parece que hay una desconfianza construida alrededor de la figura de las personas que trabajan en seguridad informática”, acota. Desconfianza que de alguna forma busca “tratar de controlar un conocimiento que al poder se le hace peligroso”.

Así, la producción del imaginario del hacker se vuelve una estrategia política: “si tenemos activistas que defienden el derecho a la privacidad, el derecho a los datos personales, el derecho a la libertad de expresión en internet, los derechos humanos en el ámbito digital, me parece que el mejor «frame» a los fines de preparar las condiciones mediáticas para legitimar estos casos de persecución pasa por la categoría de hacker. Finalmente no es que están protegiendo nada ni desarrollando herramientas para proteger la privacidad, sino que van y te hackean la computadora”, explica Adriel.

De esa manera, los activistas, las voces críticas y los disidentes políticos que desarrollan su trabajo en relación a la tecnología pueden ser fácilmente desestimados, silenciados y, como en los casos de Bini y Smaldone, perseguidos. Esto es todavía más problemático cuando, en palabras de Adriel, “buena parte del activismo de organizaciones que nada tienen que ver con lo digital, pasan por lo digital”, ahí donde la tecnología se vuelve también condición de posibilidad del disenso.

Por supuesto, el problema es todavía más complejo en tanto las mismas plataformas que permiten circular,

amplificar y compartir información relevante para la discusión y la organización de la protesta política, en sus diferentes formas, puede ser también utilizada por el poder estatal para la persecución y la criminalización de quienes participan en ella. Esta es una cuestión que hemos podido observar de manera muy clara en el convulsionado fin de año que ha tenido Chile, sumido en una gran protestas social, con movilizaciones ininterrumpidas desde el viernes 18 de octubre.

Mientras que los servicios de redes sociales han sido fundamentales para el intercambio de informaciones y, particularmente, para la denuncia de diversos atropellos a los derechos fundamentales de las y los manifestantes, especialmente a manos de Carabineros -la policía uniformada acusada de golpear, mutilar, violar y literalmente atropellar<sup>13</sup> personas en el marco de las protestas- el Gobierno está más interesado en la posibilidad de utilizar esta información para buscar responsabilidades penales entre quienes protestan e intentar sustentar disparatadas teorías sobre el origen de la revuelta.<sup>14</sup>

En ese sentido, Adriel pone el énfasis en la “des-elitización” del ámbito digital, donde “el constante acercamiento de las organizaciones que se dedican a esto con otro tipo de organizaciones -movimientos de mujeres, de género, sindicatos y demás organizaciones que tienen una lógica contestaria frente a algunas relaciones de poder” - se vuelve una necesidad.

---

13 Es el caso de Óscar Pérez, atropellado el viernes 20 de diciembre en las cercanías de la Plaza de la Dignidad. <https://www.cooperativa.cl/noticias/pais/manifestaciones/joven-atropellado-y-aplastado-por-carro-policial-esta-fuera-de-riesgo/2019-12-20/220850.html>

14 En diversas ocasiones el presidente Sebastián Piñera ha intentado imponer la tesis de que las protestas en Chile han sido instigadas por agentes extranjeros. El gobierno intentó respaldar dichas aseveraciones mediante un informe de “big data”, que ponía en el centro del descontento a famosos cantantes, humoristas y fanáticos de la música coreana, resultando en un bochornoso episodio. Para más información, ver <https://www.derechosdigitales.org/14074/el-gobierno-al-escrutinio-de-las-redes-lo-que-las-imagenes-ocultan/>

