Antonio Madrid Pérez

Vigilancia digital: antes y después del COVID-19

La crisis en la que estamos inmersos intensifica el debate acerca de qué usos hacer de los instrumentos de vigilancia digital por parte de aquellos Estados que tienen capacidad técnica para hacerla. La vigilancia digital permite geolocalizar a personas que han dado positivo por coronavirus y hacer un seguimiento de sus movimientos, permite también aplicar programas de identificación facial para complementar la geolocalización, permitiría tener acceso a la lista de contactos de las personas infectadas y conocer con quiénes interactuaron durante las últimas semanas, permite que personas informen sobre el comportamiento de otras personas o permite hacer seguimiento de las personas afectadas a partir de la información que compartan en una app sobre seguimiento de los síntomas del coronavirus.

Por una parte, la vigilancia digital puede ser un instrumento muy eficaz de control sobre la población. Sin embargo, esta misma eficacia presenta aspectos preocupantes en relación con los derechos y libertades de las personas. Por otra parte, la vigilancia digital puede ser muy eficaz si se pone al servicio de la población. Por esta dualidad de usos existe un enorme debate sobre el diseño y aplicación de las tecnologías de vigilancia digital.

China se confirma como el ejemplo más contundente de vigilancia digital del Estado sobre su población. Esta vigilancia ha sido utilizada para constreñir a la población en el cumplimiento de las normas de confinamiento. En el caso chino, el uso intensivo de la vigilancia digital ha sido posible porque el país ya se había dotado de un complejo sistema que combina tres elementos: una extensa red de cámaras instaladas en espacios públicos, la generación y explotación de enormes bases de datos, y sistemas algorítmicos que permiten acceder rápidamente a la información disponible. Además de estos recursos técnicos, la legislación china ya imponía un alto grado de control estatal sobre la población.

Situaciones excepcionales como la del COVID-19 hacen que se vuelva más urgente la pregunta acerca de qué tecnologías utilizar para combatir la propagación de la enfermedad. Por el momento, los datos disponibles indican que países como China han sido bastante más eficaces que España, Italia o Estados Unidos en frenar la expansión de la epidemia. Cuando se explican los factores que han podido contribuir a esta desigual afectación, se suele indicar, no sin reservas, el uso de la vigilancia digital como instrumento eficaz de evaluación y control de la población infectada.

En marzo de 2020, el gobierno de Israel decidió, sin pasar por el Parlamento, aplicar medidas antiterroristas a las personas que habían quedado infectadas. Se aprobó el rastreo de sus móviles con la intención de conocer qué contactos habían tenido 15 días antes y conocer también si estaban cumpliendo la orden de confinamiento **[1].**

Es muy probable que una de las consecuencias de esta crisis sea la apuesta por el incremento de la vigilancia estatal como estrategia de actuación de los Estados. Esta estrategia ya había sido impulsada en algunos Estados como instrumento de prevención de delitos o de aseguramiento de

determinadas zonas. En Gran Bretaña, por ejemplo, la policía utiliza desde hace tiempo sistemas de reconocimiento facial **[2].**

En septiembre de 2019, un tribunal de Cardiff validó el uso gubernamental de tecnologías de reconocimiento facial (Caso Edward Bridges contra CCSWP and SSHD **[3]**). El problema central que abordó la sentencia fue discernir si la policía de Gales del Sur respetaba o violaba la legalidad vigente en el uso que hacía y hace la tecnología de reconocimiento facial. La discusión se centraba en la protección de la privacidad y de los datos personales a partir del uso de esta tecnología. El tribunal británico consideró que la forma en que la policía utilizaba el reconocimiento facial no vulneraba el artículo 8 del Convenio europeo de Derechos Humanos que recoge el derecho a la vida privada de las personas.

A diferencia de Cardiff, San Francisco ha seguido un camino distinto. En mayo de 2019, esta ciudad aprobó limitaciones en la adquisición y el uso de la tecnología de reconocimiento facial. La razón por la que tomó esta decisión fue la alerta provocada por los errores en la identificación de personas, especialmente mujeres y personas con piel oscura u otros colectivos que podían ser discriminados por su origen, religión u otra característica. Esta prevención en el uso de esta tecnología de vigilancia digital se adopta en una zona que concentra buena parte de las principales compañías mundiales dedicadas a la innovación y el desarrollo tecnológico: Silicon Valley.

Ante una situación de pandemia, toda la población puede ser sospechosa de ser portadora del virus, ya sea hoy o mañana. Nadie puede asegurar: yo no lo padeceré ni lo transmitiré. Albert Camus, en *La peste* (1947), habló de lo que puede ocurrir en una pandemia. Las personas pueden mostrarse solidarias y cuidar a sus semejantes. También pueden exacerbar la violencia ya sea por odio o por miedo, o por las dos cosas. Las respuestas ante la pandemia pueden ser diferentes. La vigilancia digital se muestra como un instrumento posible que de utilizarse ha de estar sometido a información y control público, a control legal y su uso ha de ser transparente. En momentos excepcionales en que todos somos sospechosos, a unos se les puede hacer más sospechosos que a otros. Cuando finalice la crisis sanitaria y la excepción, hay que tener cuidado en no substituir la sospecha vírica por otras sospechas a las que vigilar digitalmente.

Notas:

[1] https://www.theguardian.com/world/2020/mar/17/israel-to-track-mobile-phones-of-suspected-coronavirus-cases

[2] https://www.lawsociety.org.uk/support-services/research-trends/algorithm-use-in-the-criminal-justice-system-report/

[3] Sentencia disponible en https://www.judiciary.uk/wp-content/uploads/2019/09/bridges-swp-judgment-Final03-09-19-1.pdf

?