SCIO. Revista de Filosofía, n.º 20, Julio de 2021, 63-91, ISSN: 1887-9853

EL USO DE LAS TECNOLOGÍAS PARA EL CONTROL SOCIAL POR LOS GRUPOS DE PODER

THE USE OF TECHNOLOGIES FOR SOCIAL CONTROL BY POWER GROUPS

Santiago Carrasco Díaz-Masa[a*]

Fecha de recepción y aceptación: 18 de febrero de 2021 y 10 de junio de 2021

DOI: https://doi.org/10.46583/scio_2021.20.816

Resumen: La crisis sanitaria provocada por el SARS-COV2 ha planteado la necesidad de un cierto control social por parte de los Gobiernos como medida para luchar más eficazmente contra la pandemia. Este control social puede ejercerse, entre otras formas, a través de las tecnologías y en especial las tecnologías de la informática y las comunicaciones (TIC). El abanico de posibilidades es muy amplio y recibe un tratamiento distinto, así como diferentes aplicaciones, según el régimen político, la religión o religiones y, en general, la cultura de cada país.

El control social no es una cosa nueva y lo ejercen no solo los Estados, sino también las empresas –en especial las tecnológicas– con objetivos distintos, pero quizás con mayor eficacia. Algunas de ellas basan su modelo de negocio precisamente en el control social.

Palabras clave: pandemia, tecnología, control social, política, religión.

[a] Dirección General de la Policía. Subdirección General de Logística e Innovación. Unidad de Informática y Comunicaciones. Sección de Formación.

[*] Correspondencia: Policía Nacional. Calle Julián González Segador s/n. Edificio D.E.T. Planta 7.ª. 28043 Madrid. España.

E-mail: Scarrasco74cf@policia.es

Abstract: The health crisis caused by SARS-COV2 has raised the need for a certain social control by governments as a measure to more effectively fight the pandemic. This social control can be exercised, among other ways, through technologies and especially Information and Communications Technology (ICT). The range of possibilities is very wide and receives a different treatment, as well as different applications, depending on the political regime, religion or religions and, in general, the culture of each country.

Social control is not a new thing and it is exercised not only by states, but also by companies –especially technological ones– with different objectives but perhaps with greater efficiency. Some of them base their business model precisely on social control.

Keywords: pandemic, technology, social control, politics, religion.

El control social es un ejercicio de influencia de unos actores sobre otros, utilizando herramientas que pueden ser intangibles como conjuntos de prácticas, actitudes sociales, valores morales, cultura y religión o utilizando herramientas expresamente invasivas como medios y dispositivos tecnológicos o medios violentos y coactivos. En este artículo pensaremos en el control social ejercido a través de las tecnologías, sin perder de vista en ningún momento esa utilización de valores, culturas, religiones y las prácticas invasivas, en el uso de ese vector tecnológico como herramienta para alcanzar el objetivo último.

En la literatura existente algunos autores ya advierten sobre el abuso de este control social, también en el ámbito tecnológico que los Estados, sobre todo, y también muchas grandes empresas, con fines diferentes, vienen ejerciendo sobre algunos grupos de población. Las consideraciones son diferentes y hay quien lo aplaude y quien lo denosta, como práctica maquiavélica, e incluso se discute su verdadera eficacia. De ello se han ocupado autoridades en geopolítica como el coronel Pedro Baños (Baños, 2017), Michael Morrell (Morrel, 2015), exponiendo su rentabilidad, u otros como Glen Greenwald (Greenwald, 2015), cuestionándola por momentos.

En este artículo, el autor planteará las capacidades reales de la tecnología entendida como herramienta y las posibilidades reales de llevar a cabo

las operaciones, entendiendo el término como el conjunto de acciones que ejecutar para alcanzar unos objetivos.

El uso de las tecnologías como herramienta para el control social necesita de uno o más vectores de incidencia. Es lo que en seguridad y defensa denominamos *vectores de ataque*. Desde luego, está por determinar si el control social puede ser considerado como un ataque, en el sentido negativo que la cultura occidental moderna hace del término *ataque*. La elección de dicho término no es caprichosa, sino que se adecúa perfectamente a la definición matemática de vector, pues implica que tiene una dirección y un sentido entre sus propiedades. La dirección es la línea que une al sujeto controlado con el sujeto controlador y el sentido puede ser único, si se trata de un control impuesto, o doble, si se trata de un control consentido y colaborativo.

Cuando hablamos de un control social impuesto, con un sentido único, el sujeto controlado puede ser consciente cuando es informado de que va a ser sometido a dicho control. La entidad controladora dispone de herramientas legales para ejercer ese control y se limita a informar a los ciudadanos de que va a hacerlo. Cuando hablamos de un control consentido o colaborativo, el sujeto controlado emite su consentimiento, sin el que la entidad controladora no podría ejercer dicho control por razones probablemente legales y, si además es colaborativo, el sujeto controlado asume un rol más activo, prestando algún tipo de apoyo necesario, como por ejemplo instalar una aplicación en su teléfono móvil o rellenando una encuesta. En estos dos casos, consentido y colaborativo, el vector tiene una dirección y dos sentidos.

Como en todos los sectores económicos y sociales, el desarrollo y la comercialización de productos tecnológicos tiene dos direcciones. En unos casos existe una necesidad y se desarrolla un producto a medida que pueda satisfacerla, y en otros casos una buena idea puede traducirse en un producto que después hay que vender y para lo cual es necesario crear la necesidad en los potenciales clientes, cuando esta no existe.

Así pues, las necesidades y los productos se convierten en la excusa perfecta o si se prefiere, el escenario perfecto para enmascarar el objetivo último y principal, que en muchos casos es el control social de la población, ya sea en una parte o en el total de esta. Cuando los productos desarrollados

son tecnológicos las oportunidades son casi ilimitadas para el controlador. Hablemos de algunos de estos campos.

§1. Deporte y ocio

El deportista pide herramientas que le ayuden a registrar su actividad y así mejorar su rendimiento sin poner en peligro su salud. Para ello se desarrollan aplicaciones basadas principalmente en la geolocalización por satélite (GPS) y sensores de movimiento y pulsómetros. Conectando una pulsera que registra el pulso y las vibraciones a un teléfono inteligente (*smartphone*), el deportista puede saber cuánta distancia ha recorrido, cuánto tiempo se ha ejercitado y cuáles han sido sus principales constantes vitales. Consigue así registrar y almacenar esa información para poder comparar sus entrenamientos y conocer su evolución. No le importa poner esa información en manos de los fabricantes e incluso con frecuencia la publica por su propia iniciativa para compartirla con la comunidad.

Lo interesante de este caso radica en la popularización de estas actividades, que lejos de quedarse en un ámbito minoritario han pasado a ser una saludable moda en los últimos años. A ella se ha sumado una gran parte de la población, de todo rango de edades, también en parte porque resulta muy económica y está al alcance de prácticamente todas las economías.

Si nos detenemos en el caso *Strava*, como ejemplo más mediático, nos encontramos con que el deseo de hacer deporte de los ciudadanos, y el uso masivo de esta red social y su aplicación para entrenamiento monitorizado, por cientos de miles de personas, incluidos los militares, ha facilitado a los Gobiernos extranjeros los contornos exactos de las bases militares y, en ocasiones, incluso los contingentes de estas. Cuando el mando aliado tuvo conocimiento de esta circunstancia ya hacía tiempo que observadores hostiles estaban explotando esta fuente inesperada de información para conocer los hábitos y capacidades de sus adversarios.

El experto en ciberseguridad Tobias Schneider, del Global Public Policy Institute de Berlín, investigó los mapas de calor producidos por la acumulación de la actividad de los distintos usuarios de la aplicación para descubrir

que era capaz de determinar la localización y el perfil preciso de la base militar taiwanesa desde la que se gestionan los misiles crucero que apuntan hacia China, así como los puestos de guardia y rutas de vigilancia. Nathan Ruser, del Australian Strategic Policy Institute, señaló el movimiento de diversas patrullas de vigilancia turcas y el perfil preciso de la base aérea estadounidense de Bagram, en Afganistán. Estos datos fueron publicados en perfiles de Twitter de todo el mundo y de ello se hicieron eco los principales medios de comunicación y publicaciones especializadas[1].

Así, vemos cómo, mientras que aplicaciones de *fitness y running* se mejoran sistemáticamente por las empresas del sector para diseñar y adaptar sus productos a los requerimientos del mercado, sin que los usuarios sean conscientes realmente de la cantidad y calidad de la información que ellos mismos, voluntariamente, están aportando, las autoridades también diseñan o adaptan sus sistemas de recopilación de información a estas aplicaciones y a las redes sociales a las que están vinculadas. Dos caras de una misma moneda.

Las aplicaciones de ocio y servicios, como Trivago*,* permiten a las grandes compañías hoteleras, de restauración o servicios conocer las preferencias de los clientes, las oportunidades de mejora en sus productos, las tendencias y los movimientos de los usuarios. Esto último comprende una oportunidad interesantísima, pues permite prever los movimientos de grupos sociales de unas zonas a otras, de unos barrios a otros, e incluso permite forzar estos movimientos en función de intereses, por ejemplo, inmobiliarios. ¿Dónde es más barato instalar un local de una famosa franquicia de comida rápida? También permite a los Gobiernos y a las empresas conocer parámetros económicos interesantes y luchar contra el fraude, por poner algunos ejemplos.

Así, por ejemplo, las empresas de seguros descubren numerosos fraudes en declaraciones de siniestros, investigando la actividad del declarante en las RR. SS.[2] (Girolimetto, 2018), o las agencias tributarias de países como

[1] Estos datos fueron publicados en perfiles de Twitter de todo el mundo y de ello se hicieron eco los principales medios de comunicación y publicaciones especializadas. Así, por ejemplo, «Strava: cómo una aplicación de deportes dejó al descubierto secretos de bases militares de Estados Unidos», en *BBC News*, del 29 de enero de 2018.

[2] Fabián Antonio Girolimetto (2018). INESE Wilmintong Risk & Compilance. Disponible en: <https://acortar.link/bjIyM>.

Francia o España[3], que investigan en las RR. SS. buscando indicios de fraude fiscal por parte de los ciudadanos, incluso se pueden usar algoritmos e inteligencia artificial sobre las RR. SS. para destapar casos de fraude fiscal[4] (González, 2020), identificando relaciones familiares y estableciendo así los verdaderos controles sobre las empresas y la ingeniería fiscal agresiva para evadir impuestos.

§2. Emergencias. Ayuda y rescate

Otra oportunidad para el control social es el manejo de la seguridad. No entendemos el término *manejo* como manipulación, sino como tratamiento del servicio, con la honorable intención de mejorarlo. La seguridad debe entenderse como un estado del individuo y de la colectividad. Las personas necesitan sentirse seguras y la sociedad necesita de la seguridad para prosperar. Es un hecho que las organizaciones terroristas sustentan su actividad y sus objetivos en el fomento de la inseguridad, o si se quiere, en el menoscabo de la seguridad. Algunos Estados son calificados de Estados terroristas y algunas organizaciones terroristas se califican a sí mismas como Estados[5]

[3] El proyecto de Ley de Finanzas para 2020 del Gobierno francés, en su artículo 9, prevé que las administraciones Fiscal y de Aduanas recolecten información que los ciudadanos publiquen en las RR. SS., para ver si existen discordancias entre lo que declaran y el tipo de vida que llevan. Asunción Serena (2019). *La Voz de Galicia*.

La Agencia Tributaria española analiza las redes sociales en busca de defraudadores, según manifestó el director general de la Agencia, Santiago Menéndez, en el Congreso de los Diputados en febrero de 2015. Jesús Servulo González. *El país*, 20 de febrero de 2015. Disponible en: <https://elpais.com/economia/2015/02/19/actualidad/1424366635_632028.html>.

[4] Ignacio González y Alfonso Mateos (octubre de 2020). *Observatorio Social de La Caixa*.

[5] Michael J. Morell (2015). *La gran guerra de nuestro tiempo*, p. 334.

La Casa Blanca (EE. UU.) (abril de 2019). Se anuncia la calificación de la Guardia Revolucionaria de Irán como "grupo terrorista". Disponible en: <https://www.whitehouse.gov/>. En el momento de la publicación de este trabajo, la nueva Administración de Joe Biden ha archivado algunas noticias de la Administración Trump, y se ha hallado esta noticia en el siguiente enlace: <https://acortar.link/EaEae>.

El Departamento de Estado (abril de 2019) declara a la Guardia Revolucionaria de Irán como organización terrorista y acusa al Gobierno iraní de financiar y apoyar el terrorismo, acusándole directamente de ser responsable de la muerte de al menos 603 soldados estadounidenses. Disponible en: <https://www.state.gov/>. La noticia ha sido archivada por la nueva Administración de Joe Biden en el siguiente enlace: <https://acortar.link/vnAzR>.

(Morell, 2015). Esta necesidad de alcanzar la seguridad tiene como derivada la oportunidad para el control social. En el tema que nos ocupa, a través de las aplicaciones de emergencias, ayuda y rescate.

Entre ellas están algunas gubernamentales como la española Alertcops[6], que permite a los usuarios denunciar en tiempo real y de forma discreta todo tipo de hechos delictivos o situaciones de emergencia. El usuario debe registrarse con todos sus datos personales reales, de forma que las fuerzas de seguridad conocen en tiempo real quién denuncia, qué hechos denuncia y dónde se producen estos hechos. Se trata de un control social consentido y cooperativo que, sin duda alguna, contribuye a la mejora de la sociedad porque, más allá de los casos concretos que se denuncian, permite a las autoridades conocer la situación de la seguridad y así planificar y optimizar los recursos. Es un vector de doble sentido porque también da la posibilidad a las autoridades de emitir avisos a la población, ejerciendo así la capacidad de influir en los comportamientos en un espacio concreto o de forma masiva. Por ejemplo, avisando de un incendio, del corte de una carretera o de una manifestación multitudinaria.

Esta herramienta no está pensada como primer objetivo para el control social, aunque resulta inevitable que los administradores adquieran esa capacidad. Sin embargo, desde el punto de vista ético, se dan dos circunstancias que hacen especialmente recomendable el uso de estas herramientas. Por un lado, está la participación voluntaria de la ciudadanía en la mejora de la seguridad colectiva, más allá del uso legítimamente egoísta para la seguridad propia. Por otro, está la simbiosis que se produce entre la Administración y el administrado, en tanto que la participación no solo es voluntaria, sino que el control se produce de manera transparente y el administrado es informado continuamente de cualquier acción que se tome sobre él y tiene la capacidad de cancelar su actividad dentro de la aplicación, o rectificarla, en cualquier momento.

No todo el espectro de población valora positivamente este tipo de herramientas, por razones precisamente éticas. Muchos ciudadanos recelan de las posibles intenciones de la Administración, consideran que siempre hay razones ocultas y oscuras detrás de estas iniciativas y mantienen la creencia

[6] <https://alertcops.ses.mir.es/mialertcops/>.

de que prevalece el interés por el control social, mientras que el servicio de seguridad ofrecido no es más que la excusa o tapadera.

Esta forma de pensar o actitud no es del todo criticable. El sentimiento de tranquilidad y seguridad que se puede experimentar con el uso de esta aplicación no tiene por qué ser mayor o más importante que el sentimiento de angustia o zozobra que se puede sentir al saberse continuamente observado, localizado y monitorizado. Dicho esto, mi propia experiencia profesional, y también personal, me induce a pensar que es muy habitual que se oculten intereses espurios e intenciones antisociales o delictivas en el rechazo a ciertas formas de control social. Quienes no tienen nada que ocultar no suelen manifestar temor ante un interrogatorio.

En todo caso, y aun siendo lícitos los diversos sentimientos personales ante inferencias externas en el espacio de la intimidad, el sacrificio personal y la solidaridad, pese a renunciar a determinado confort y a ciertas cuotas de intimidad, son moralmente más plausibles que el egoísmo y el individualismo.

Consideremos un caso real como ejemplo gráfico y sencillo para la reflexión sobre esta última afirmación: en una reunión de vecinos uno de los puntos del orden del día pretende decidir sobre la conveniencia o no de instalar un sistema de videovigilancia en el portal, debido a que se han producido varios incidentes que han afectado al mobiliario y a algunos vecinos. Una madre de familia relata cómo un desconocido asaltó a su hija adolescente en el portal y, por supuesto, vota a favor. Esta madre no se plantea si el sistema va a servir para otra cosa que no sea disuadir a los delincuentes de actuar. No se plantea quién va a tener acceso a las imágenes y qué uso van a hacer de ellas, seguramente porque solo va a hacer uso del portal como lugar de tránsito obligado entre la vía pública y su domicilio y no prevé situaciones incómodas para su intimidad. Además, confía en el sistema y en la ley, dando por seguro el uso y mantenimiento legal del sistema y de la información. Otra vecina vota en contra de la propuesta porque no confía en los administradores del sistema y da por sentado que las personas con acceso a las imágenes grabadas van a verlas de manera sistemática, ocurran o no incidentes que lo justifiquen y por simple diversión. Defiende su derecho a la intimidad y la salvaguarda de su imagen a capa y espada. Tras un debate intenso, esgrime el argumento de que tiene derecho a llegar bebida a su casa y que no se quede grabado en

un vídeo que luego pueda servir para la mofa. Al final resulta que lo que subyace es un sentimiento de culpa o de vergüenza ante un comportamiento que la propia persona considera moralmente cuestionable y, por lo tanto, prefiere mantenerlo en su intimidad, incluso a costa de que su actitud egoísta implique posibles perjuicios graves para la comunidad. Ambos sentimientos son lícitos y ambos son igual de intensos, pero uno de ellos implica un sacrificio personal y renuncias en favor de la comunidad y el otro no. Lo que cabe plantearse es cuál es el objetivo del control, si es evitar incidentes o mofarse de los vecinos que han abusado del alcohol.

En realidad, cualquier aplicación para un teléfono móvil o un ordenador puede constituir un sistema de control social encubierto. En las clases sobre seguridad en telefonía móvil suele incluirse un epígrafe dedicado a los niveles de los permisos que las aplicaciones requieren del sistema operativo para su ejecución. En función del nivel concedido, la aplicación tendrá acceso a los recursos del sistema que necesite y le sean concedidos. Por ejemplo, acceso al micrófono, al GPS, a las llamadas telefónicas, a la cámara, a la galería de imágenes, a los SMS, a los archivos y a un largo etcétera de recursos tanto de *software* como de *hardware*.

Los niveles 3 y 4 son difíciles de conseguir porque necesitan certificados digitales que solo emite el fabricante del teléfono o del sistema operativo. Son precisamente en ellos en los que se consigue el acceso a los elementos más críticos de cara a la seguridad y privacidad. En cuanto a los niveles más bajos, el 1 y el 2, se consiguen mediante los permisos del usuario casi sistemáticamente.

Sin embargo, no es imposible que una aplicación adquiera niveles superiores. Todo dependerá del cuidado que ponga el usuario y de la capacidad de persuasión que tenga el proveedor de las aplicaciones. Como casi siempre, con técnicas de ingeniería social se puede conseguir casi cualquier cosa y es frecuente que el usuario final conceda los permisos pulsando un botón cuando se le requiere. Si el proveedor de la aplicación no es un delincuente sino una Administración, es relativamente fácil que el usuario conceda todo tipo de permisos.

Así sucede, por ejemplo, cuando se quiere disponer de un servicio de cita médica a través de la aplicación móvil de la Consejería de Salud correspondiente. En este caso, es muy probable que el usuario, durante el registro, conceda todos los permisos que se le soliciten, como, por ejemplo, la

geolocalización. Sin embargo, este no parece un permiso imprescindible para solicitar una cita con el médico de familia, mientras que sí es un dato muy interesante para el ejercicio del control social.

§3. Navegación

Uno de los sectores que más adeptos ha logrado en los últimos años es la navegación: el uso de dispositivos para movernos de un punto a otro del espacio geográfico. En un primer momento apenas se podían encontrar algunas pocas marcas con dispositivos específicos, mientras que hoy los dispositivos GPS se encuentran integrados incluso en los teléfonos móviles de precios más populares.

Merece la pena detenerse en este punto para analizar el papel que juega el precio de las cosas en el control social a través de las tecnologías. Especialmente si se pretende que este control social se ejerza con la participación voluntaria de los ciudadanos.

Como se ha visto anteriormente, el control social puede ser impuesto o colaborativo. En este último caso, cabe plantearse quién lo paga. Si lo paga el controlador, al usuario controlado le puede ser indiferente el precio que tenga, siempre y cuando el controlador sea una entidad privada. En el caso de que el controlador sea la Administración, entonces ya no resulta indiferente para el ciudadano, porque lo paga él indirectamente. El precio pasa a ser un asunto relevante. No digamos si el precio del vector usado se repercute directamente en el sujeto controlado. Cuando hablamos de control social a través de medios tecnológicos, la probabilidad de conseguir los objetivos de control es inversamente proporcional al coste que se repercuta en el ciudadano.

El caso extremo es cuando el control es impuesto y además lo paga el sujeto controlado. Parece realmente difícil que esto pueda ocurrir, pero seguramente no es así. Si lo planteamos desde una perspectiva europea, democrática y socialmente avanzada, no parece fácil que el control social pueda ser impuesto porque seguramente afectará a normativas rigurosas de protección de datos y también de derechos fundamentales. No solamente dentro de cada Estado, sino que también en las asociaciones de Estados o en las organizaciones supranacionales –como la Unión Europea– existen normativas comunes que

afectan a los miembros, a sus empresas y a sus ciudadanos. En un escenario en el que predomina el Estado de derecho dentro de modelos democráticos no parece, en principio, que se pueda imponer el control social, y mucho menos que el coste se le imponga. No es, sin embargo, imposible, como se ha podido comprobar en una situación casi imprevisible, que como mínimo ha sorprendido a la mayoría de los Estados miembros de la Unión. Se trata de la aparición de un inesperado factor externo que ha empujado a la toma de decisiones impensables en una situación de normalidad. La enfermedad de la COVID-19 ha desempolvado figuras legales que no se recordaban en Europa desde la Segunda Guerra Mundial. Todos los Estados han aprobado medidas excepcionales en base a regulaciones como el estado de alarma o similares, que permiten limitar o incluso anular algunos derechos fundamentales como la libre circulación.

Por increíble que pueda parecer, esta situación ha permitido a los Estados más modernos, democráticos, sociales y progresistas, y aún más increíblemente a los Gobiernos más liberales, eliminar o limitar temporalmente derechos como el trabajo o el libre comercio.

En algún caso, merecedor de estudio, incluso se ha llegado a limitar el derecho a la información y la libertad de opinión. En España, que pasa por ser uno de los Estados más progresistas dentro de un ámbito geopolítico tan democrático y garantista como la Unión Europea, durante el estado de alarma los sistemas tecnológicos de control social han llegado a convertirse en herramientas decisivas, que se han considerado imprescindibles para controlar y manejar la opinión de los ciudadanos de cara a la lucha contra la pandemia.

Durante la llamada "primera ola de la pandemia", el general jefe del Estado Mayor de la Guardia Civil reconoció, en una de las ruedas de prensa que se realizaban diariamente en aquellos momentos, que la Jefatura del Servicio de Información del Instituto Armado estaba trabajando para "minimizar el clima contrario al Gobierno"[7]. Esta afirmación, que fue rápidamente matizada por miembros del Gobierno y posteriormente por él mismo, pone de manifiesto

[7] Pablo Muñoz (2020). El Jefe de Estado Mayor dice que la Guardia Civil trabaja para "minimizar" las críticas al Gobierno. *ABC*, 19 de abril de 2020. Disponible en: <https://acortar.link/24bue>.

que existe un interés del Gobierno por ejercer un cierto control sobre la opinión pública en lo que se refiere a la propia gestión gubernamental de la pandemia.

Entendemos, por lo tanto, que ninguna de las tres formas de control social (impuesto, consentido o colaborativo) es imposible, ni siquiera en un Estado comprometido con el respeto a los derechos civiles.

En estas circunstancias, la navegación se convierte en uno de los principales vectores para ejercer este control social en cualquiera de sus formas.

Los navegadores son facilitados por los propios fabricantes de los sistemas operativos móviles y son entregados de manera gratuita a los usuarios. No puede ser más barato. Los navegadores de pago incorporan mejoras de usabilidad y funciones adicionales que pueden ser del gusto de los consumidores, y aun así lo hacen a un precio cada vez menor. Navegadores que costaban 100 euros anuales en los inicios de la distribución masiva de *smartphones* han pasado a costar apenas unas decenas de euros con licencias para toda la vida y actualizaciones gratuitas. Existen navegadores con licencias perpetuas y actualización continua por apenas 20 euros. Se puede considerar que están al alcance de cualquiera.

En todo caso, si no se desea pagar por este servicio, se pueden tener estos dispositivos de forma gratuita con el único requisito de contar con acceso a internet.

Una novedad importantísima que han incorporado todos los navegadores en los últimos años es la navegación colaborativa. La colaboración de los ciudadanos facilita que el navegador pueda saber dónde están los atascos, las obras o cualquier incidencia sobre la vía en tiempo real. Para conseguirlo es necesario que los usuarios faciliten ciertos permisos, que casi siempre se otorgan inconscientemente a pesar de que la ley impone que se emitan avisos en la pantalla. Lo habitual es que se acepten las condiciones de uso sin llegar a leerlas. Con estos permisos la aplicación accede a los datos de posición y los envía a los servidores en tiempo real para que analicen constantemente dónde hay mayor concentración de dispositivos, a qué velocidad se mueven, hacia dónde, etc., de manera que el sistema sabe lo que está pasando en la vía e informa a los usuarios de forma gráfica y sonora.

Las aplicaciones de navegación suponen un gran avance en lo social y también en lo económico. Permiten, por ejemplo, que las mercancías lleguen

por carretera mucho antes y con menor coste en horas de trabajo, combustible y mantenimiento de los vehículos. Pero, desde luego, ofrecen una gran oportunidad para el control social. El uso del navegador puede ser voluntario, si se trata de un desplazamiento, pero generalmente se ejecutan también en segundo plano, con lo que la corporación recibe la información sin conocimiento del usuario.

§4. Radar COVID. El caso general y el caso catalán

La comunidad científica coincide unánimemente en la necesidad de conocer y rastrear los casos positivos de COVID-19 para atajar la propagación del virus causante de la enfermedad. La mejor manera, sin duda, es conocer los contactos sociales de estos positivos y automatizar los procesos con el uso de tecnologías de las comunicaciones, técnicas de Big Data y de trazabilidad. Este es el sentido que se presenta como principal para la aplicación Radar COVID, que se ha propuesto por el Gobierno para su uso en todo el territorio.

Es interesante ver cómo la Administración ha presentado esta aplicación de cara a la opinión pública, para lo que nos puede servir el texto utilizado por la Consejería de Sanidad de la Comunidad de Madrid:

> La app Radar Covid es una aplicación gratuita, con carácter confidencial, que permite al ciudadano conocer su grado de exposición al virus, así como alertarlo en el caso de que haya mantenido un contacto estrecho con una persona positiva a la infección, para, de esta manera, avisar a la mayor brevedad de la exposición de riesgo y la adopción de medidas preventivas.
>
> El ciudadano interesado en utilizar la aplicación tiene que descargarla en el móvil, activar el bluetooth y permitir que funcione de manera anónima. La app Radar Covid garantiza el anonimato y confidencialidad de los usuarios, así como la no geolocalización o identificación del número de teléfono.
>
> La alerta por COVID-19 se inicia cuando un caso confirmado, y a su vez usuario de la aplicación, recibe a través de SMS un código o clave para que la introduzca en Radar Covid. A continuación, la aplicación envía una alerta de manera anónima a las personas con las que haya estado en contacto estrecho y cuenten también con esta app. A estos se les indicará, a su

> vez, que se pongan en contacto con el teléfono del Centro de Atención al Paciente (CAP) de la Consejería de Sanidad para el seguimiento sanitario correspondiente: 900 102 112[8].

La Administración conoce la preocupación que los usuarios tienen por su intimidad y sabe que, con la legislación vigente en España, necesita que colaboren voluntariamente en el uso de una aplicación que es intrusiva. Siempre que se recopilan datos relacionados con las enfermedades concretas que sufre una persona surgen reticencias por parte de los ciudadanos. En el caso de la COVID-19, existe además el miedo al estigma social de padecer una enfermedad sin cura y de desarrollo incierto, sobre la que ha existido una gran confusión y desinformación. Nadie quiere ser señalado y todos tienen miedo al rechazo y la marginación social.

Es curioso que en el texto que publica la Administración se haga mayor hincapié en los beneficios personales que la aplicación traerá a quien la instale que al impacto que tendrá en el control de la pandemia y, por lo tanto, el beneficio colectivo y, desde luego, se vuelca el mayor esfuerzo informativo en explicar al usuario cómo se garantizan sus derechos de privacidad.

Expresamente se quiere tranquilizar al ciudadano diciéndole que:

1. La aplicación es gratuita. La Administración es consciente de que el precio es relevante, como hemos comentado anteriormente, y que para que el usuario colabore en un sistema de control social colaborativo este tiene que ser barato o, preferiblemente, gratuito.
2. Garantiza el anonimato y la confidencialidad de los usuarios.
3. No geolocaliza.
4. No identifica el número de teléfono.

De estas cuatro afirmaciones solo la primera es cierta, y ni siquiera del todo: la aplicación se financia con fondos públicos que finalmente pagan todos los contribuyentes, aunque ciertamente no hay que pagar por ella en el momento de instalarla.

[8] Comunidad de Madrid (octubre de 2020). «Actualidad». Disponible en: <https://acortar.link/6lgje>.

Para descargar e instalar una aplicación en un *smartphone* es necesario estar registrado en un repositorio tipo Google Play o App Store. Es cierto que esto puede hacerse con perfiles falsos o bajo cobertura, pero esto no es posible de ninguna manera para acceder a la red de comunicaciones. La Administración debería prometer que "no va a recopilar datos de identidad de los usuarios", pero no debería decir que garantiza el anonimato de estos. No puede garantizar la confidencialidad al tiempo que recomienda dirigirse al centro de atención al paciente para comunicar un positivo o el contacto con él. El ciudadano debe saber que, desde el punto de vista estrictamente técnico, la confidencialidad absoluta en las redes móviles no existe y que, llegado el caso, la Administración puede acceder a todos sus datos con la preceptiva autorización judicial. El estado de alarma constituye una herramienta que podría permitir a la Administración dictar normas en este sentido, al tratarse de una limitación de los derechos fundamentales. Si la propagación de la enfermedad llegara a ciertos extremos, la Administración podría solicitar acceso a esos datos con fines probablemente justificados desde el punto de vista ético, para avisar o incluso confinar obligatoriamente a los ciudadanos que hayan estado en contacto con el virus. Sin duda, se trata de un planteamiento extremo pero no imposible, por lo que indicar que la confidencialidad está garantizada es como mínimo inexacto.

Afirma la Administración en su anuncio que no se geolocaliza a los usuarios, lo que desde el punto de vista técnico es falso. Precisamente, el éxito de la aplicación se basa en conocer qué terminales están cerca de otros pertenecientes a (o que son portados por) ciudadanos contagiados o que han estado en contacto con el virus. Para ello se requiere activar el dispositivo *bluetooth* del teléfono. Cuando se tiene suficiente cercanía como para que el sistema identifique al otro terminal, el servidor central relaciona ambos terminales y los relaciona con otros muchos. Esta técnica es, en definitiva, una demarcación territorial de rebaños. Como mínimo, en el hipotético caso de que fuera cierto que no se geolocalizan los terminales desde el punto de vista de coordenadas geográficas, lo que es innegable es que se construye una red de posicionamiento relativo entre ellos. La red sabe quién ha estado cerca de quién. Por supuesto, y por las razones expuestas en el punto anterior, la Administración podría tener la autorización legal de geolocalizar con exactitud cada terminal

en todo momento. Para ello basta con que un juez considere que hay un fin que lo justifica.

Desde el punto de vista ético, teniendo como premisa el interés general de la comunidad y dando como cierto que España constituye un estado de derecho, democrático, con separación de poderes y que garantiza los derechos civiles de sus ciudadanos, no parece razonable que la Administración tenga que persuadir a sus ciudadanos de que no va a hacer un uso espurio o inmoral de sus capacidades, así como indicarles que el uso de los datos será meramente temporal, con compromiso de su destrucción, y con el único objeto de la lucha contra la pandemia. Sí cabe cuestionar la actitud de los ciudadanos que anteponen su interés particular por el anonimato a un bien común tan importante como evitar la expansión de la epidemia, por un lado, y, por otro, la de la Administración que, incapaz de convencer con argumentos y razones suficientes, esconde la realidad y no actúa con la transparencia que le sería exigible.

La Administración es plenamente consciente del control social que ejerce con esta aplicación y también del enorme peso que este podría tener para su popularidad, hasta el punto de que las distintas administraciones disputan sobre su uso. El Gobierno de la Comunidad Autónoma de Cataluña, consciente de estos hechos, ha desarrollado su propia aplicación equivalente a Radar COVID, llamada ContacteCovid.cat[9]. Es cierto que esta aplicación centraliza sus datos con la propia del Gobierno de España, pero recomienda a sus ciudadanos que instalen y utilicen la propia de la Administración catalana.

El Gobierno de la Generalitat, posiblemente priorizando objetivos políticos, considera importantes dos cuestiones en lo que se refiere a esta herramienta. La primera es la necesidad constante de transmitir una capacidad clara de manejar cualquier situación con los medios propios e independencia total de la ayuda del Estado. Se trata de transmitir una imagen de autosuficiencia política y de independencia *de facto* respecto al Estado español. La segunda es la conveniencia de la explotación del potencial del control social que esta herramienta ofrece para los objetivos políticos propios, consciente de la ventaja informativa que obtendría de cara a los resultados de las políticas

[9] Generalitat de Catalunya (octubre de 2020). Disponible en: <https://acortar.link/DbZTC>.

sanitarias que planear y ejecutar, con el consiguiente aumento del prestigio y popularidad para el Gobierno autonómico entre sus adeptos. Parece éticamente reprobable esta actitud egoísta e irresponsable de anteponer los intereses políticos al interés general de su población, sean o no independentistas los afectados, sobre un interés moralmente más elevado como es la salud. Esta afirmación, que tal vez pudiera parecer sesgada o partidista, se sustenta en un hecho que es irrefutable y que no es otro que lo innecesario de la aplicación catalana cuando ya existe otra que es aceptada y recomendada por el resto de administraciones, generales y locales.

§5. Los sistemas del hogar

Al contrario de lo que pueda parecer, las tecnologías que permiten ejercer el control social no son una novedad. Desde hace ya algunos años, muchos hogares disponen de sistemas conectados a redes que permiten un control social de los usuarios abonados. De hecho, algunos de estos sistemas están pensados principalmente para ello, aprovechando otras oportunidades técnicas y comerciales que ofrecen estas tecnologías.

Un ejemplo pueden ser los sistemas de alarma y vigilancia domésticos. Estos sistemas están conectados normalmente a una central de alarmas. Se protege la identidad del abonado y se le ofrece un servicio discreto. Sin embargo, cualquier incidente de una determinada gravedad que sea comprobado debe ser comunicado a las fuerzas del orden, lo que permite obtener información de forma rápida y hacer planes en el nivel estratégico.

Pero donde realmente está el salto cualitativo más importante en el control social soportado en tecnologías de uso doméstico es en los contadores inteligentes de las compañías eléctricas, gas y agua. Las oportunidades de control social que estos sistemas ofrecen son casi ilimitadas. El objetivo primario que la compañía pretende alcanzar es contar con un sistema que le permita facturar los servicios consumidos con exactitud y oportunidad, es decir, en el momento pactado, lo que se conoce como consumo real y no estimado, además de ahorrar costes de personal al evitar tener que desplazar operarios a realizar las lecturas. Pero otra consecuencia es que, a través del registro de

consumo que la compañía recibe en tiempo real mediante su propia red, es posible saber cuándo hay gente en el domicilio, cuánta gente hay e incluso qué están haciendo, porque el consumo indica si están viendo un televisor, usando un ordenador, poniendo una lavadora o planchando, cuántas lámparas hay encendidas, etc. Del mismo modo, ampliando una visión imaginaria del edificio, es posible saber qué domicilios están ocupados en ese momento, por cuánta gente y qué están haciendo. Lo mismo por calles, barrios o poblaciones enteras. De nuevo, nos encontramos con una oportunidad de control social, que sin duda se está ejerciendo, y que se encuentra en manos de compañías privadas.

Muchas son compañías internacionales que operan en distintos países, lo que provoca que el conocimiento y la compilación de todos estos datos tengan también repercusiones en el ámbito de lo político.

Las grandes compañías energéticas tienen, por tanto, una gran capacidad de control social a nivel global, pueden tomar decisiones estratégicas que afectan a la economía mundial y, desde luego, condicionan la capacidad política de los Estados en la toma de decisiones. Esto supone que las compañías disponen de una información que ni siquiera tienen los Gobiernos de los Estados en los que operan, salvo que haya una cooperación activa entre el Gobierno y la compañía. No es descabellado pensar que estas compañías colaboren con los Gobiernos de los países donde tienen sus sedes principales, lo que podría considerarse como una clara injerencia de unas potencias en los asuntos internos de otras.

Los principios éticos por los que se rigen los Estados son muy diferentes dependiendo de factores culturales, religiosos y políticos, generalmente relacionados con el espacio geográfico donde se ubican. En la historia reciente hay casos documentados, juzgados y condenados, y muchos otros conocidos pero impunes, de abusos de poder ejercidos por los Gobiernos con la colaboración activa de grandes compañías tecnológicas. Cuando un gobierno no tiene reparos en abusar de su población en cuestiones de derechos fundamentales, mucho menos los tendrá en un asunto como el control social masivo y constante, que es una actividad menos pública y traumática para el individuo en primera instancia, aunque a largo plazo tenga consecuencias igualmente graves para él y para la colectividad. El control social, cuando se trata de

Estados no democráticos según los estándares occidentales, se ejerce generalmente para la perpetuación del régimen.

§6. El SARS-COV-2. ¿Es el virus un sistema de control social encubierto?

No es posible abordar este tema, desde un punto de vista tecnológico, sin acudir, aunque sea tangencialmente, a una cierta "teoría de la conspiración".

En los primeros días de la pandemia de la COVID-19, el principal debate que se producía en todos los lugares de reunión no era si sería más o menos grave la enfermedad. Tampoco era si duraría mucho o poco. Ni siquiera era si la cura llegaría pronto o cuánto costaría. En aquellos días, el principal debate entre la gente corriente era: ¿de dónde ha salido el virus?, ¿lo ha creado alguien o de verdad viene de algún animal exótico? Los especialistas de los medios de comunicación social aseguran que un virus no puede crearse desde cero. Sí que aseguran, sin embargo, que un virus ya existente en un repositorio (un animal) puede ser artificialmente modificado para que tenga unos determinados comportamientos, se adapte a ciertas circunstancias o presente características precisas. Siempre tendremos la duda de si efectivamente el virus procede de un animal y saltó a los humanos en algún lugar, por razones estrictamente naturales, o si, por el contrario, se trata de algún tipo de experimento con virus modificados y el producto procede de un laboratorio. En este segundo caso, es probable que tampoco lleguemos a saber nunca si se trató de un accidente y hubo un escape indeseado o, por el contrario, se difundió deliberadamente. Todas las agencias de inteligencia del mundo se hacen estas preguntas. Lo más probable, y desde luego lo más razonable, es lo primero, pero no vamos a renunciar a lo segundo, pues nos permite hacer un interesante ejercicio de análisis.

En seguridad y defensa decimos que cuando se produce un hecho criminal y no sabemos por dónde empezar a analizarlo lo primero que hay que hacer es "seguir la pista del dinero".

Cabría, por tanto, hacerse algunas preguntas. Lo fácil sería recurrir directamente a la hipótesis de culpabilidad del Gobierno chino, pero es más honesto realizar las preguntas y que el lector elija sus respuestas.

- ¿Quién no tenía almacenados suficientes recursos materiales para hacer frente a una oleada de contagios tan grande? Nos referimos a mascarillas, respiradores, plazas hospitalarias, etc.
- ¿Quién sí tenía almacenados suficientes recursos materiales para hacer frente a una oleada de contagios tan grande? Incluso la capacidad de construir hospitales en plazos asombrosamente cortos.
- ¿Quién tenía capacidad de producir esos recursos a tales niveles como para cubrir sus propias necesidades y abastecer al resto del mundo? ¿Quién ganó muchísimo dinero, por tanto?
- ¿Quién está abasteciendo de estos materiales de forma masiva a todos los mercados?
- ¿Qué pasó con los mercados de valores y quién tenía tanto dinero disponible como para aprovechar la circunstancia y comprar todo tipo de empresas?
- ¿Quién tiene más proyectos, en paralelo, de vacunas? ¿Podría tratarse de un virus de laboratorio cuya vacuna ya existiera en el momento de la propagación de la enfermedad y que se distribuirá cuando convenga?
- ¿Quién tiene mayor capacidad de producir masivamente medicamentos y, en el futuro, las vacunas de manera más económica y competitiva?

Después de responderse a esas preguntas, lo siguiente es preguntarse cómo ha influido la pandemia en el control social ejercido por los Estados. Desde luego, la respuesta es sencilla, si se plantea con relación a países con regímenes totalitarios. Los países comunistas de Asia han ejercido ese control de forma impuesta –sin contar con la voluntariedad de los ciudadanos– con todo tipo de medidas, incluidas las tecnológicas, incluso han obligado a los individuos a instalar aplicaciones de control social en sus móviles. Estos gobiernos no se plantean cuestiones éticas sobre el control social impuesto y, en muchas ocasiones, tampoco los ciudadanos, porque forma parte ya de su cultura, de su forma de entender la pertenencia social. Por eso aceptan con resignación,

salvo una resistencia minoritaria, todo tipo de medidas, incluso extremas, mientras que en las democracias occidentales la renuncia a los derechos fundamentales en pos de un aumento de la seguridad es una tensión clásica.

El virus en sí mismo podría comportar una medida tecnológica con el objetivo de aumentar el control social sobre la población de una forma masiva. Sin embargo, hay otra derivada que llevaría, siguiendo esta teoría conspirativa, al aumento de este control con el uso de otro producto tecnológico para satisfacer una necesidad de los clientes, en este caso creada *ex profeso*. Siguiendo uno de los modelos expuestos al inicio de este artículo, se quiere vender un producto que no es requerido por los clientes y entonces es necesario crear la necesidad. Si se quiere vender una vacuna que sirva como sistema tecnológico para el control social, primero habrá que difundir de forma masiva un virus que haga necesaria esta vacuna. La vacuna por sí misma no permite el control de una forma continuada. Para ello sería necesario inocular en los pacientes algún tipo de dispositivo, con la excusa de la vacuna, que permita la monitorización continuada en el tiempo.

No han sido pocas las personas, de mayor o menor importancia social, las que se han adherido a esta teoría[10]. Teniendo en cuenta los diversos factores implicados, económicos, sociales, políticos y legales, esta es una posibilidad muy remota. Es muy improbable que pudiera realizarse una operación de tal magnitud, pero cabe plantearse si es técnicamente posible.

Es muy improbable porque las sociedades democráticas occidentales no lo tolerarían y se producirían sin duda graves incidentes, a escala mundial, que desembocarían en crisis políticas sin precedentes. Ocurriría, sin duda alguna, porque una operación de tal magnitud no puede ocultarse.

¿Es imposible instalar un chip en el cuerpo humano que permita el control social a gran escala? Desde luego, técnicamente es posible. Desde hace muchos años viene haciéndose con normalidad en todo tipo de animales

[10] En España se produjo un episodio muy mediático que tuvo como protagonista al presidente de la Universidad Católica de San Antonio de Murcia (UCAM), D. José Luis Mendoza, que aseguró en un discurso público que determinadas organizaciones y personas muy poderosas pretenden controlar la libertad de las personas inoculando un chip a través de la vacuna contra el SARS-COV-2. Véase J. García (2020). El chip de la vacuna del Covid para controlar: dice el presidente de la Universidad Católica. *El Español* (16 de junio). Disponible en: <https://acortar.link/QSoz9> y <https://dai.ly/x7uhuj8>.

domésticos. También en explotaciones ganaderas, con fines conservacionistas y para investigaciones zoológicas. Lo que no es posible es hacerlo discretamente. Sí es posible insertar un chip sin que lo sepa el paciente, pero no es posible ocultarlo a corto plazo.

¿Qué tipo de tecnología es la que permite hacer una cosa así? Es necesario un dispositivo de identificación similar al que se usa con las mascotas. Se trata de dispositivos RFID, los denominados "Chip Espía" por Katrine Albretch y Liz McIntyre, de la *Citizens Against Marking, Chipping and Tracking* (Albretch, 2006)[11].

Un dispositivo RFID (*Radio Frequency Identification Device*) es un circuito electrónico de identificación por radiofrecuencia que tiene una pequeña capacidad de almacenamiento donde se registran los datos del sujeto portador, así como un sistema de transmisión sin alimentación interna (llamado «etiqueta pasiva»). No nos vamos a detener demasiado en complejas cuestiones técnicas, pero sí explicaremos su funcionamiento. Cuando el aparato de lectura se acerca suficientemente al chip, alrededor de 10 cm, le induce una pequeña corriente eléctrica que es suficiente para que el receptor le devuelva la información almacenada en su pequeña memoria. De este modo, se necesita tener instalado en el cuerpo el dispositivo RFID y un aparato lector muy cercano.

Estos dispositivos están ya muy extendidos en nuestra sociedad, implementados en las tarjetas bancarias (*Contact Less*), en las tarjetas de identificación para acceso a instalaciones, en los chips de las mascotas y un largo etcétera cada día mayor. Si se observa el chip integrado en una tarjeta bancaria o el DNI electrónico, o la pequeña cápsula que se inyecta a un gato, podría pensarse que es imposible instalarlo en el cuerpo humano, pero nada más lejos de la realidad. En el año 2006, la compañía japonesa Hitachi desarrolló un dispositivo pasivo denominado μ-Chip con un tamaño de 0,15 × 0,15 mm sin antena, más delgado que una hoja de papel (7,5 μm); y en el año 2007, un dispositivo aún menor, de 0,05 × 0,05 mm, y lo suficientemente delgado como

[11] Katherine Albrecht (2006). *Chips Espias (Spychips): Cómo las grandes corporaciones y el gobierno planean monitorear cada uno de sus pasos con RFID*. Nashville: Grupo Nelson, Harper Collins Christian Publishing.

para poder estar integrado dentro de la hoja de papel. Este dispositivo podría discretamente ser instalado a través de una inyección subcutánea. Cabría preguntarse si tendría algún tipo de efecto secundario, si sería reabsorbido por el torrente sanguíneo a causa de su pequeño tamaño y otras preguntas de tipo médico, pero sin duda podría ser instalado sin conocimiento del sujeto receptor. Hasta este punto podría avalarse técnicamente esta teoría, que el autor de este artículo insiste en considerar muy improbable.

El segundo componente del sistema, los receptores, que sería el equivalente al aparato TPV de los comercios o al lector de las puertas de seguridad, se tendría que desplegar por millones en lugares donde se garantizara que los ciudadanos van a pasar lo suficientemente cerca como para que pueda realizarse la lectura. Además, tendrían que estar conectados a una inmensa red de comunicaciones. Esta red ya existe, pero no el despliegue de lectores, que no es imposible.

El uso de este tipo de tecnología constituiría una intromisión en la intimidad muy superior al que permiten las aplicaciones que se han descrito anteriormente en este artículo, y su potencial para el control social por parte de los Gobiernos es enorme.

Una vez visto el aspecto puramente técnico, que conlleva grandes dificultades de ejecución, lo que realmente hace muy improbable esta teoría es la imposibilidad de hacerlo sin la colaboración de los ciudadanos. No se puede ocultar una señal de radio y no se puede ocultar un dispositivo RFID en el cuerpo, por pequeño que este sea, a una resonancia magnética o una ecografía rutinaria en un centro de salud. No se tardaría ni un solo día en que quedase desvelado. El estallido social sería de proporciones incalculables, hasta el punto de que el colapso judicial sería insignificante en comparación con los disturbios violentos que sin duda se producirían.

Otras tecnologías que pudieran ofrecer esta oportunidad de control social basadas en implantación de dispositivos en el cuerpo humano, como podrían ser los *nanobots*, biochips o similares, son hoy por hoy productos de ciencia ficción, que probablemente estarán disponibles en el futuro, pero no creemos que cercano. Al mismo tiempo, es de esperar que también se desarrolle una tecnología de detección y diagnóstico que impida su difusión encubierta o discreta.

En todo caso, y como vemos, el control social en Occidente pasará por el modelo colaborativo, lo que puede ayudar a que se desarrolle con absoluta transparencia y control legal.

§7. Sociedades y culturas

El control social como fenómeno es tremendamente diferente en los distintos países, dependiendo de su organización política, su cultura o incluso su religión. Así pues, hay una gran diferencia en cómo toleran este hecho los ciudadanos asiáticos, los musulmanes, los europeos o las poblaciones indígenas.

En China, como gran potencia que ya es, enormemente poblada y muy tecnificada, el control social es continuo y va en aumento. El Gobierno chino legisla en función de un delicado equilibrio entre garantizar la perpetuidad del régimen y contener a una población cada día más influida por otras formas de pensar. China es un país que ha apostado por la industria tecnológica como modelo económico de expansión y de crecimiento. Como consecuencia, su población dispone de esta tecnología a precios muy bajos y la consume de forma casi compulsiva. El Gobierno se esfuerza enormemente en limitar la libertad de información y ejerce la censura con descaro. La censura y el control de la información ya son de suyo un medio de control social, pero lo que tal vez más sorprende de la sociedad china es la enorme fuerza que ha alcanzado el control social a través de la tecnología. Estos elementos tecnológicos se utilizan a favor de los intereses de un régimen que, seguramente, los seguirá empleando y mejorando por mucho tiempo y sin grandes dificultades, debido a las características culturales de una población que es en general disciplinada y sumisa, acostumbrada a las normas de la colmena. Esta visión podría ser extrapolable a todo el sudeste asiático y, en lo importante, también a Japón, que es una sociedad extremadamente tecnificada en la que los ciudadanos viven la tecnología con pasión y cuya economía depende en buena medida de este sector. Si bien el Estado es mucho más democrático y transparente, la cultura japonesa se presta con gusto al control social como herramienta para adquirir estabilidad y seguridad. La diferencia está en la voluntariedad en el país nipón, mientras que China opta por la imposición.

En Occidente la cuestión es mucho más compleja. El control social es mucho más discutido y requiere necesariamente de la colaboración de los ciudadanos. No solo la cultura occidental, en especial la anglosajona, es mucho más celosa de sus derechos civiles, sino que los defiende con fuerza y se dota de los medios legales para garantizarlos.

Podría pensarse que los Estados no democráticos, tal como lo entendemos en Europa, deberían tender hacia modelos de sociedad política occidentales, pero esto es algo que está por ver.

La influencia de la religión es muy fuerte en el mundo islámico, y afecta a los comportamientos sociales y a la determinación de las políticas interiores, las políticas educativas, etc. También tiene una fuerte influencia en la percepción de la tecnología, que sufre un fuerte rechazo que, atendiendo a la evolución de sus líderes, no parece que cambiará sustancialmente en los próximos años. Por ese motivo, el uso de la tecnología como mecanismo de control social es todavía muy limitado, y se ejerce más bien a través de instituciones que influyen en la sociedad de forma directa (Gobierno) o a través de la difusión de ideas y modos de vida (comunidad religiosa).

§8. Empresas *vs*. Estados

El desarrollo tecnológico ya no depende tanto de los Estados como de las empresas. Históricamente, los grandes avances tecnológicos han estado directamente relacionados con la guerra y el desarrollo de nuevas armas y sistemas de defensa. En estos tiempos, sobre todo en Occidente, los Estados han delegado esta función en las grandes empresas tecnológicas, si bien en algunos países estas son controladas en mayor o menor medida por los Gobiernos. De esta manera, la capacidad de controlar a la población por medio de la tecnología está principalmente al alcance de las empresas. Por este motivo, los Gobiernos realizan grandes esfuerzos para mantener un cierto grado de control sobre las empresas, y en todo caso se aseguran la colaboración de estas a través de diferentes medios, que pueden ir desde la legislación impositiva hasta la cooperación comercial (Lefébure, 2014).

En los últimos años, el control social ha recaído masivamente en unas pocas empresas tecnológicas que libran su propia guerra fría en paralelo a los Estados a los que sirven. El pequeño grupo conformado por Apple, Huawei, Microsoft, Amazon, AliExpress, Google, Samsung y Xiaomi aglutina probablemente la casi totalidad del mercado tecnológico mundial.

Huawei se encuentra en medio de una cruenta guerra comercial entre Estados Unidos y China, y se ha convertido en un posible instrumento del Gobierno chino para ejercer el control social sobre el mundo entero, además de obtener información directa de todos sus competidores. Huawei ejerce casi el monopolio de las redes de telecomunicaciones mundiales. El gran público lo reconocerá únicamente por los teléfonos móviles baratos de buena calidad que oferta, pero Huawei es además el principal proveedor mundial de equipos de red. Telefónica, sin ir más lejos, ha construido toda su red 4G con equipos suministrados por Huawei. El resto de grandes compañías de telecomunicaciones ha hecho normalmente lo mismo. EE. UU, ante la invasión global de este fabricante, ha iniciado una guerra tecnológica y comercial, no solo por el miedo a que el control social de su país quede en manos de China, sino porque esta situación pone en una grave tesitura a su industria.

Amazon y AliExpress controlan el mercado mundial del comercio electrónico, de la logística y pronto de los contenidos multimedia, y cada uno de estos actores servirá a los intereses de las dos grandes potencias mundiales.

Xiaomi, Samsung y Apple son los modelos tecnológicos preeminentes en cuanto a terminales de usuario, que son sin duda el vehículo de transporte más cercano al individuo para llevar la información a donde corresponda.

En cuanto al tratamiento de la información, hay tres grandes modelos que acaparan el mercado: Apple, Microsoft y Google.

Apple basa su modelo en la venta de dispositivos (*hardware*) de gran calidad y exclusivos. Impide deliberadamente la compatibilidad con terceros a cambio de ofrecer mayor longevidad, calidad de materiales y fiabilidad. Todos los usuarios de Apple se manifiestan muy satisfechos con sus productos.

Microsoft no vende *hardware*, sino sistemas operativos y aplicaciones. De hecho, sus sistemas y aplicaciones son compatibles con todo tipo de máquinas y durante muchos años ha estado facilitando que los usuarios instalen

sus productos bordeando la legalidad de las licencias. Es como el traficante que ofrece droga gratis las primeras veces para empezar a cobrarla cuando el drogadicto ya no puede parar de consumir. Ha llevado a la mayoría a su redil durante años, permitiendo el pirateo hasta hoy. Dispone así de una enorme masa de clientes y de información.

Google no vende programas ni sistemas operativos, de hecho, los regala. Tanto Android como todas sus herramientas, que son masivamente utilizadas por todos los ciudadanos del planeta, son gratuitas y están en continua actualización. Tampoco vende las máquinas sobre las que se instalan. Ofrece todos sus servicios de forma gratuita y, a cambio, comercia con sus clientes. Comercia con su información personal, su actividad, sus aficiones y, en definitiva, con sus vidas. Todo ello legalmente y con el consentimiento y la colaboración de sus clientes, que aceptan con agrado las condiciones del contrato debido a su gratuidad.

¿Por qué Google y todas las empresas con las que colabora nos envían publicidad de la tienda que tenemos más cerca? Porque sabe dónde estamos, sabe hacia dónde vamos y a qué velocidad, e incluso sabe lo que estamos buscando. Esos datos, de claro control social sobre toda la población, los envía con su correspondiente factura a cualquier empresa interesada en vendernos su producto. Durante muchos años, uno de sus principales clientes era el Gobierno de Estados Unidos (Greenwald, 2015)[12].

§9. Control social, información y desinformación

Desde el punto de vista del uso de la tecnología, el control social permite obtener información de los ciudadanos que es de interés para la toma de decisiones en el ámbito del Gobierno y del mercado y, a su vez, permite influir en las decisiones de los individuos. Por ejemplo, creando corrientes de opinión. Los medios de comunicación social son un excelente vehículo que, apoyándose adecuadamente en la tecnología, tienen una gran capacidad de control social.

[12] G. Greenwald (2015). *Snowden. Sin un lugar donde esconderse*.

Los Gobiernos no tienen el menor reparo en utilizar su propia influencia sobre los medios de comunicación social y sobre las redes sociales, cuando no su control total, para alcanzar sus objetivos. En la era de las televisiones y de las plataformas digitales, los Gobiernos se aseguran la colaboración de estas para difundir su mensaje. La capacidad de las televisiones para influir en la población es inmensa. En España la polarización política de los distintos grupos mediáticos ha tenido influencia directa en los resultados de las últimas elecciones generales y, a nivel mundial, Gobiernos tan distintos como el iraní, el saudí, el chino, el norteamericano y el ruso se aseguran de disponer de medios de comunicación que alcancen a escala global a su público para difundir su mensaje y crear su corriente de opinión. Internamente, esto solo ocurre, como es esperable, en los Estados democráticos donde la pluralidad es mayor[13].

Muchos Estados, como Rusia, además de contar con grandes medios de comunicación instalados en muchos países extranjeros (como Russia Today y Sputnik), han volcado sus esfuerzos también en las redes sociales. Lo mismo hacen los pseudo-Estados, principalmente representados por grupos terroristas del estilo de Dáesh, Al Qaeda, Boko Haram y otros muchos, porque en el mundo virtual y deslocalizado es más fácil y barato difundir sus mensajes y crear realidades paralelas.

Esto también nos debe llevar a reflexionar sobre la desinformación, que es una estrategia dirigida a alterar la percepción de la realidad de la opinión pública. No solo se puede modificar el comportamiento de otros a través de una información seleccionada, sino también sesgándola o, directamente, creando información falsa. Aparece así el control social mediante la desinformación, aunque pueda parecer paradójico, y para ello son indispensables las nuevas tecnologías.

[13] Algunos medios de comunicación y agencias de noticias gubernamentales más influyentes:
Rusia: TASS (agencia de noticias estatal). Russia Today y Sputnik. Grupos de comunicación.
EE. UU. Associated Press (AP) y United Press International (UPI), agencias de noticias. CNN, grupo de comunicación.
Reino Unido: Reuters, agencia de noticias. BBC, grupo de comunicación.
Francia: France Press, agencia de noticias.
China: Xinhua News Agency, agencia de noticias.
Qatar: Al Jazeera, referente del mundo árabe suní.
Irán: Press TV.
España e Hispanoamérica: EFE, agencia de noticias.

Referencias bibliográficas

Albrecht, K. (2006). *Spychips*. Nueva York: Plume.

Baños, P. (2017). *Así se domina el mundo*. Barcelona: Ariel.

Girolimetto, F. (2018). El uso de las redes sociales para prevenir el fraude en materia de seguros. *INESE*, 8 de marzo. Disponible en: <https://acortar.link/bjIyM>.

González, I., Mateos, A. (2020). ¿Se puede destapar el fraude fiscal con algoritmos? *Observatorio Social de la Caixa*. Disponible en: <https://acortar.link/rsbM2>.

Greenwald, G. (2015). *No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State*. Nueva York: Picator.

Lefébure, A. (2014). *L'affaire Snowden : Comment les Etats-Unis espionnent le monde*. París: La Découverte.

Morell, M., Harlow, B. (2015). *The Great War of Our Time*. Nueva York: Twelve.