Comisión 4. Comisión de Libertades Civiles, Justicia y Asuntos de Interior.
La búsqueda de inmunidad digital frente a la pandemia. Eficacia, privacidad y vigilancia.

La Unión Europea es uno de los mejores embajadores mundiales de la democracia. A pesar de la complejidad de las estructuras y organismos en los que se asienta el club comunitario, la Unión Europea tiene metas muy dispares que persiguen, sin embargo, lograr el mismo objetivo: proteger los valores democráticos. La protección de los ciudadanos europeos frente a amenazas de distinta índole es uno de los mayores desafíos a los que se enfrenta la UE diariamente y, en gran parte, su razón de ser; no en vano, el origen de la Unión Europea era garantizar la paz en el continente. Sin embargo, en determinadas circunstancias extraordinarias, esta protección no es tan visible. En otras, como parece sugerir la pandemia ocasionada por el COVID-19, el ciudadano tiene que elegir entre dos protecciones que, de repente, se excluyen: la salud, o la privacidad.

La búsqueda de inmunidad digital frente a la pandemia: eficacia, privacidad y vigilancia

Hemos naturalizado tanto llevar un dispositivo siempre con nosotros, el móvil, que a veces parece una extensión más que un aparato electrónico. La tecnología de las telecomunicaciones, y los móviles, han evolucionado tanto en los últimos años que, en la mayor parte de los casos, lo que llevamos en la mano tiene más bien la potencia y las funcionalidades de un ordenador en miniatura.

Lo cierto es que los dispositivos móviles nos hacen la vida más fácil, en términos generales. Gracias a ellos, y a Internet, no solamente tenemos un acceso inmediato a todo lo que ocurre en el mundo. Podemos, también, conectar y mantener conversaciones instantáneas con otras personas, pedir comida a domicilio o hacer la compra, comprar entradas de cine o cualquier otro espectáculo, revisar el correo electrónico, hacer transferencias o consultar nuestras cuentas a través de la banca online. Podemos incluso ver series, escuchar la radio o hacer ejercicio. Los móviles nos mantienen conectados al mundo que nos rodea en todo momento y nos permiten, junto con otros dispositivos,

sentirnos más cerca de las personas en circunstancias excepcionales, como la pandemia por el COVID-19. Gracias a los móviles, quienes viven lejos de sus familias o quienes no han podido salir de sus hogares durante meses por el confinamiento han podido seguir relacionándose, aunque haya sido a través de una pantalla.

Precisamente, y debido a la pandemia mundial, los móviles se han colocado en el centro de muchas estrategias gubernamentales para poder contener el virus. En algunos países, tanto europeos como extracomunitarios, se han desarrollado aplicaciones que permiten saber no solamente qué persona ha dado positivo a COVID-19, si no también con quién ha estado en contacto el enfermo y en qué lugares ha estado. La tecnología al servicio ciudadano para ayudar a combatir una pandemia por una emergencia sanitaria tiene, *a priori*, muchas ventajas, pero también tiene inconvenientes, y es necesario entender qué peligros encierran estas aplicaciones y el uso de ellas.

Por un lado, el rastreo de casos y contagios a través de una aplicación que cada ciudadano tenga en su móvil quita peso y, en consecuencia, presión, al personal sanitario y hospitales. Si bien el rastreo manual puede ser, en algunos casos, más efectivo, no podemos olvidar que de esta tarea también se encargan quienes ya llevan acumulados muchas horas de trabajo, mucho estrés por las condiciones del desempeño de sus funciones, y mucho cansancio. En sus propias jornadas, el personal sanitario tiene que atender a los pacientes (ya sea de forma telefónica o presencial) y hacer un rastreo manual de los posibles contagios; en consecuencia, se corre el riesgo de que la efectividad o la productividad, y el propio bienestar de los trabajadores sanitarios, estén en peligro.

Otra ventaja del rastreo de contagios a través de los móviles es que tiene en cuenta las multitudes. Esto quiere decir que el rastreo manual de personas en contacto con un positivo en COVID-19 es fácil cuando esta última solo ha estado con gente cercana o conocida. Sin embargo, este rastreo resulta imposible cuando ese no es el escenario. Y, aunque en la actualidad las multitudes son, por lo general, una circunstancia improbable, en un futuro a medio o a largo plazo es una variable importante a tener en cuenta, por lo complicado de mantener a una población confinada o semi-confinada de forma permanente en el tiempo.

Por otro lado, sin embargo, estas aplicaciones móviles, en ocasiones, podrían no ser del todo efectivas: es el caso de aquellas que incluyen un cuestionario de auto-diagnóstico como punto de partida, algo que no puede ser comparado ni con un diagnóstico profesional ni con una prueba médica. No funcionan, además, de forma aislada: son solamente un refuerzo en una situación en la que los diagnósticos clínicos y otro tipo de rastreo sean la norma. Algunas de estas aplicaciones, además, plantean serios problemas para la privacidad de los usuarios, de los ciudadanos, por varios motivos. El primero es que estas aplicaciones de rastreo funcionan en su mayoría con Bluetooth, un método de transmisión de datos poco fiable, puesto que no es seguro ni es efectivo a ciertas distancias. Esa falta de seguridad deja vulnerables a los dispositivos móviles, donde muchas personas guardan datos de acceso, información privada o incluso confidencial. En segundo lugar, se trata de aplicaciones que usan la geolocalización para saber dónde estás en todo momento, con qué personas has estado, a qué hora y en qué condiciones. El uso de estos datos para tratar de frenar una pandemia, para combatir una emergencia sanitaria, es una ventaja e incluso un avance tecnológico, pero habría que tener cuidado con las libertades que se ponen en riesgo cuando se hace uso de esos datos, especialmente tras la pandemia. El acceso de los gobiernos a la geolocalización permanente de los individuos es una herramienta de gran poder, que da una gran capacidad de control y vigilancia a los ciudadanos. Usado de un modo erróneo, puede contradecir los principios democráticos y vulnerar las libertades del individuo.

No se puede olvidar, además, que aunque algunas de estas aplicaciones han sido desarrolladas y promovidas por diversos gobiernos, ninguna de ellas se sustenta en datos gubernamentales. Todas estas aplicaciones comparten el mismo punto de partida: los datos de trazado de movilidad que grandes empresas tecnológicas, como Apple, Google o Microsoft ya tenían en su poder. Esto quiere decir que, por un lado, empresas privadas estarían facilitando a los gobiernos datos personales que están en el limbo de lo legal por lo extraordinario de la situación. Por el otro, que nadie sabe a ciencia cierta a dónde van a ir a parar esos datos tras la pandemia pero, en el peor de los casos, esas mismas empresas privadas tendrán datos sanitarios y sobre la salud de los individuos que, de otro modo, a lo mejor a nivel individual muchos no habrían querido compartir.

De esto último se desprende el peligro más notable: el que pone en riesgo la inmunidad de los individuos, y la libertad de movimiento sin prejuicio de su estado de salud en situaciones normales. En China, por ejemplo, los individuos tienen que mostrar con el móvil su estado de salud en relación a la COVID-19 para poder acceder a ciertos establecimientos o restaurantes. En Corea del Sur, la aplicación de geolocalización permite a las autoridades realizar una videollamada a cualquier hora del día (o noche) para comprobar tu estado, o que una persona está realmente donde dice estar (esto es, que no ha dejado el móvil en un sitio físico distinto a donde se encuentra la persona). Ante la falta de respuesta, las autoridades se reservan el derecho de acudir al domicilio del individuo y, en todo caso, entrar.

¿Qué pasaría si este tipo de datos sobre la salud de los individuos fuera un requisito, tras la pandemia, para el acceso a ciertos servicios?

*** Cuestiones para iniciar la reflexión en la Comisión 4**

- ¿Debería ser la gestión de la COVID-19 una estrategia nacional o europea?
- ¿Cuál es el principal desafío al que se enfrenta la UE en términos tecnológicos a la hora del uso de estas aplicaciones?
- Se insiste en que la descarga de las aplicaciones del rastreo de contagios debe ser, en todo caso, voluntario. Sin embargo, un estudio de la universidad de Oxford concluye que estas herramientas solo son efectivas cuando las usa el 60% de la población. ¿Cómo se podría gestionar esto a nivel europeo?
- ¿Sería posible el desarrollo de una aplicación de rastreo de uso europeo, que combinara los datos de todos los países? ¿Cómo podría la Unión Europea hacer frente a esta posibilidad?
- ¿De qué forma puede asegurarse la Unión Europea de que estos datos se usarán solamente durante la pandemia, si depende de los datos de inicio de empresas privadas?

Enlaces de interés:

Estudio de la universidad de Oxford sobre el éxito de las aplicaciones de rastreo: https://www.research.ox.ac.uk/Article/2020-04-16-digital-contact-tracing-can-slow-or-even-stop-coronavirus-transmission-and-ease-us-out-of-lockdown

Aplicaciones para rastrear el coronavirus, ¿solución o problema de privacidad?: https://www.lavanguardia.com/vida/junior-report/20200424/48669453804/aplicaciones-para-rastrear-el-coronavirus-solucion-o-problema-de-privacidad.html

Tracking and tracing COVID: Protecting privacy and data while using apps and biometrics: https://www.oecd.org/coronavirus/policy-responses/tracking-and-tracing-covid-protecting-privacy-and-data-while-using-apps-and-biometrics-8f394636/

How to use COVID tracking apps and still protect your privacy: https://www.forbes.com/sites/helenalbert/2020/06/19/how-to-use-covid-19-tracking-apps-and-still-protect-your-privacy/#2f7158912e20