DERECHOS FUNDAMENTALES, PRIVACIDAD Y APLICACIONES MÓVILES MÉDICAS*

Lori ANDREWS**

I. Presentación

Hoy en día, los pacientes tienen más poder que nunca para enfrentarse a problemas de salud y bienestar. Pueden buscar información sobre salud online, administrar su salud a través de aplicaciones médicas, y hasta jugar a juegos relacionados con la medicina. Los padres pueden subir una foto de su niño enfermo a su página de Facebook y pedir ayuda para diagnosticarlo (AITKEN Y LYLE, 2015).

Pero si alguna vez usted investigó los efectos alternativos de una medicación online, mandó un mail a un pariente sobre su salud, indicó que le gusta una organización de servicios de salud en su página de Facebook o descargó una aplicación médica, es probable que recopiladores de datos hayan almacenado esa información sin su conocimiento ni consentimiento.

---

* Ponencia presentada en el marco del Séptimo Encuentro Anual de Lectores para la Justicia, titulado "Cómo leemos y cómo nos leen", el cual tuvo lugar el 8 de noviembre de 2017 en la Facultad de Derecho de la Universidad de Buenos Aires. Traducción al español por Josefina del Rosario Lago.

** *Lori Andrews is a Distinguished Professor of Law at Chicago-Kent College of Law, Illinois Institute of Technology, and Director of IIT's Institute for Science, Law and Technology. She has published widely on internet privacy, including her latest book, I Know Who You Are and I Saw What You Did: Social Networks and the Death of Privacy (2013).*

Professor Andrews has been an adviser on medical technologies to the U.S. Congress, the World Health Organization, the National Institutes of Health, the U.S. Department of Health and Human Services, the Institute of Medicine of the U.S. National Academy of Sciences, and several foreign nations, including the Emirate of Dubai, the French National Assembly, and G8 Science Ministers. She received her B.A. summa cum laude from Yale College and her J.D. from Yale Law School.

Luego de esto, las presunciones que los recopiladores realizan sobre su salud son vendidas a empleadores, aseguradoras, agentes hipotecarios o terceros que pueden usarlas para realizar un trato discriminatorio contra usted. En una ocasión, un asegurador compró información sobre la salud de aproximadamente 3 millones de personas a un recopilador de datos (WIECZNER, 2013).

A nivel global, se espera que el negocio de la medicina móvil alcance los $132.2 mil millones para 2023 (P&S MARKET RESEARCH, 2018). ¿Cómo se puede regular este mercado emergente asegurando los derechos fundamentales? En la mayoría de los casos, las leyes y protocolos que existen hoy en día sobre la privacidad no protegen la información ingresada a las aplicaciones móviles.

En el Institute for Science, Law, and Technology en IIT Chicago-Kent College of Law realizamos una serie de estudios sobre aplicaciones móviles médicas. En los Estados Unidos, el 58% de los usuarios de smartphones han descargado alguna vez una aplicación sobre bienestar o salud (KREBS Y DUNCAN, 2015). Estas aplicaciones son programas de *software* con finalidades médicas que se puede usar usados en *smartphones*, *tablets* u otros aparatos electrónicos con acceso a Internet. Estas aplicaciones móviles médicas pueden ayudar a sus usuarios a diagnosticar, monitorear, administrar, tratar y prevenir problemas de salud y enfermedades (AITKEN Y LYLE, 2015). En algunas ocasiones, las aplicaciones suelen tomar el lugar de un doctor (FEDERAL TRADE COMMISSION LAW SERVICES, 2015). Si bien poseen beneficios, también conllevan riesgos, especialmente en cuanto a daños en la salud y cuestiones de privacidad.

En esta columna se discutirán nuestros estudios en aplicaciones médicas. Hemos analizado políticas de privacidad, descripciones de los permisos de los desarrolladores de las aplicaciones, y hemos rastreado a dónde las aplicaciones envían la información efectivamente. Usándolos en conjunto, Charles Proxy, Wireshark, Cygwin y Wakelock Detector nos permitieron interceptar todas las transmisiones entrantes y salientes, desencriptar transmisiones fácilmente encriptadas y determinar qué funciones de la aplicación eran ejecutadas en el dispositivo.

Analizamos un total de 211 aplicaciones médicas diseñadas para ayudar a los usuarios a controlar su diabetes, algunas de las cuales inclusive indicaban a los pacientes cuánta insulina tomar. Encontramos problemas en la calidad cuando las aplicaciones recomendaban administración de dosis sin tomar en cuenta las actividades que el usuario realizaba, cuál era su peso u otra información relevante.

Asimismo, encontramos una falta de privacidad, dado que sólo el 19% de las aplicaciones estudiadas tenían políticas de privacidad. Realizamos un estudio profundizado

sobre una muestra aleatoria de 65 aplicaciones para la diabetes en las cuales se observó una extracción secreta de información para ser compartida con terceras partes. El 86% de estas 65 aplicaciones colocaban *cookies* de rastreo en el dispositivo. El 76% de las aplicaciones sin políticas de privacidad enviaban información de los usuarios a recolectores de datos, mientras que esto sucedía en el 79% de las aplicaciones con políticas de privacidad. El hecho de que la aplicación tuviera una política de privacidad no se correspondía significativamente con la probabilidad de que la privacidad del usuario fuera vulnerada.

También realizamos un estudio sobre aplicaciones psiquiátricas, que requieren que los usuarios revelen información aún más potencialmente estigmatizante. De nuevo, encontramos problemas en la calidad y la privacidad. Por ejemplo, el 23% de las aplicaciones sobre bipolaridad pedía a los usuarios que indicaran sus medicaciones y las dosis consumidas para que pudieran ser aconsejados sobre probables interacciones negativas de las drogas. Cuando señalamos medicamentos que, tomados al mismo tiempo, habrían producido una interacción farmacológica fatal, sólo un tercio (33%) de las aplicaciones nos alertaron sobre la combinación potencialmente peligrosa. El otro 67% no dio aviso de que tomar esas dos drogas juntas podrían dañar o resultar en la muerte del usuario. Ninguna de las aplicaciones para controlar la ingesta de medicamentos nos alertó cuando indicamos la ingesta de una dosis letal de Litio (6000 mg). De hecho, una de las aplicaciones inclusive mostró un aviso promocionando un descuento especial para el usuario en la compra de Litio.

Sólo el 33% de las aplicaciones sobre bipolaridad tenían políticas de privacidad. El 70% divulgaba la información a empresas de marketing y análisis de datos.

II. Posibles cambios en las políticas

La información sobre las condiciones de salud de los pacientes se protege en los consultorios médicos por dos razones: para que los pacientes puedan ser honestos con los profesionales y así recibir el tratamiento adecuado, y para que no se vean discriminados en base a sus condiciones de salud. Esas mismas preocupaciones existen en el mundo *online*. Estudios muestran que las personas son reticentes a revelar información sobre su salud si conocen cuán vulnerable puede ser *online* (inclusive en situaciones en las que contar su estado de salud podría ayudarlos). Los actos discriminatorios florecen cuando la información online sobre la salud es vendida. Si usted usa una aplicación para la diabetes o publicó en un foro online sobre depresión, puede que sea rechazado en una entrevista de trabajo y nunca sepa por qué.

Una solución puede ser la divulgación obligatoria a los consumidores, que requiere que las aplicaciones avisen a los usuarios qué harán con la información obtenida. Pero,

¿quién lee los términos de servicio? Investigadores de Carnegie-Mellon concluyeron que le tomaría 30 días hábiles por año a una persona leer las políticas de privacidad de cada servicio online que utiliza de forma habitual (MCDONALD Y CRANOR, 2008). La mayoría de las personas sólo cliquean "aceptar".

Una mejor solución para proteger el derecho fundamental a la privacidad de los usuarios de aplicaciones médicas sería prohibir a los desarrolladores de las aplicaciones usar la información sobre la salud de los consumidores para marketing y prohibirles divulgar esta información a terceras partes distintas a los proveedores de salud de los consumidores.

Bibliografía

AITKEN, M. y LYLE, J. (2015) "Patient Adoption of mHealth: Use, Evidence and Remaining Barriers to Mainstream Acceptance", IMS Institute for Healthcare Informatics, septiembre 2015. Consultado en [https://www.iqvia.com/-/media/iqvia/pdfs/institute-reports/patient-adoption-of-mhealth.pdf?la=en&hash=B3ACFA8ADDB143F29EAC0C33D533B C5D7AABD689] el 07/08/2018.

FEDERAL TRADE COMMISSION LAW SERVICES (2015) "A Cancer Detecting Mobile App? FTC Says No There's Not an App for That", FTC Law, 23 de Abril, 2015. Consultado en [http://www.ftclaw.com/2015/04/ftc-vs-mole-detective-and-melapp/] el 07/08/2018.

KREBS, P. y DUNCAN, D. T. (2015) "Health App Use Among US Mobile Phone Owners: A National Survey", JMIR Mhealth Uhealth, N°4, Vol. 3, e101. Consultado en [http://mhealth.jmir.org/2015/4/e101/] el 07/08/2018.

MCDONALD A. M. y CRANOR L. F. (2008) "The Cost of Reading Privacy Policies", I/S: A Journal of Law and Policy for the Information Society, N° 3, Vol. 4, pp. 543-568. Consultado en [http://lorrie.cranor.org/pubs/readingPolicyCost-authorDraft.pdf] el 07/08/2018.

P&S MARKET RESEARCH (2018) "mHealth Market Growing with the Increasing Demand for Patient-Centric Healthcare: P&S Market Research", Global Newswire, 30 de mayo, 2018. Consultado en [https://globenewswire.com/news-release/2018/05/30/1514212/0/en/mHealth-Market-Growing-with-the-Increasing-Demand-for-Patient-Centric-Healthcare-P-S-Market-Research.html] el 16/07/2018.

WIECZNER, J. (2013) "How the Insurer Knows You Just Stocked Up on Ice Cream and Beer", The Wall Street Journal, 25 de febrero, 2013. Consultado en [https://www.wsj.com/articles/SB10001424127887323384604578326151014237898] el 07/08/2018.