CENTRO DE ESTUDIOS INTERNACIONALES
GILBERTO BOSQUES
ANÁLISIS E INVESTIGACIÓN

EL IMPACTO GLOBAL DE LA REGULACIÓN EUROPEA EN MATERIA DE DATOS PERSONALES

10 DE MAYO DE 2018

NOTA DE COYUNTURA

Imagen: Carolyn Kaster/Reuters

En 2016, la Unión Europea aprobó su Reglamento General de Protección de Datos y otorgó dos años como periodo de implementación para que las empresas interesadas tuvieran tiempo de adaptar sus nuevas políticas. Este periodo concluye el 25 de mayo, cuando entra en vigor el nuevo reglamento que contempla sanciones mucho mayores a las previas, así como lineamientos específicos para lidiar con brechas de seguridad y filtraciones. Aunque sin duda serán los ciudadanos europeos los que más se verán beneficiados por estos nuevos lineamientos, los ciudadanos del resto del mundo también lo harán por el alcance de la legislación, la cual contempla que debe resguardarse la información personal de todo usuario sin importar su nacionalidad o ubicación geográfica. La entrada en vigor del reglamento no podría ser más oportuna, dado que ocurre poco después que se desatara el escándalo de la filtración de datos de Cambridge Analytica así como la comparecencia de Mark Zuckerberg, CEO de Facebook, ante el Congreso estadounidense. En esta última se subrayó la enorme distancia que existe entre cómo suponen los usuarios que operan las redes sociales con sus datos y la realidad de sus modelos de negocio. Sin duda, el Reglamento General de Protección de Datos es el primer paso para cerrar filas entre ficciones y realidades.

The impact of Europe's data protection regulation on the rest of the world

In 2016, the European Union approved the General Data Protection Regulation and gave all companies who collect, store and process data a two-year window to adapt to new policies. Said period ends on May 25th, when the new policy will officially come into effect. This new regulation includes much heavier fines and penalties than the previous one, as well as more specific guidelines to deal with security violations and data breaches. Even though European citizens will undoubtedly be the ones to reap most of the benefits of this new legislation, citizens from across the world will also benefit since the EU specifically states that personal data must be protected regardless of the citizen's nationality or geolocation. Furthermore, this new regulation could not have come at a better time, since the Cambridge Analytica scandal broke and Facebook's CEO, Mark Zuckerberg, made his first appearance before the US Congress only weeks ago. Zuckerberg's hearing highlighted the enormous distance between how users think social networks work with their information and the reality of their business models. Undoubtedly, the General Data Protection Regulation is the first step in confronting a new reality.

Introducción

El próximo 25 de mayo de 2018 entrará en vigor el Reglamento General de Protección de Datos (RGPD) de la Unión Europea, el cual cambiará la manera en la cual se podrá recolectar, conservar y procesar datos personales.[1] Además de la introducción de ciertos nuevos controles, lo importante de esta regulación es que también tendrá un impacto en otros países. En particular el RGPD contempla cambios a la manera en la que operan gigantes del internet incluyendo *Facebook* y *Google*. Desde el escándalo del mal uso de datos por parte de la compañía *Cambridge Analytica* y *Facebook*, los llamados para regular el uso de cierta información en internet se han incrementado. El RGPD europeo bien podría significar el primer paso a nivel mundial, en particular porque su aplicación va más allá de las fronteras europeas y éstas aplicarán también en nuestro país. Toda empresa que haya sido constituida u opere en territorio europeo estará sujeta al RGPD, por lo cual todos los titanes del internet tendrán que adaptar sus modelos.[2]

Según la Unión Europea, la legislación busca "lidiar con las realidades" de la presencia de los datos en la era del internet, así como "proveer certidumbre legal para individuos y organizaciones que procesan datos y una mayor protección para el individuo en general".[3] La UE considera además que, "el procesamiento de datos personales debería de estar diseñado para servir a la humanidad" y que el incremento de datos personales entre actores públicos y privados requiere mantenerse a la vanguardia de los avances tecnológicos para asegurar "un alto nivel de protección" así como el libre movimiento de los datos personales.[4] El objetivo de la regulación es "contribuir a la plena realización de un espacio de libertad, seguridad y justicia" así como impulsar el progreso económico y social teniendo en cuenta siempre el bienestar de las personas físicas.[5]

La coincidencia de que esta nueva regulación se ponga en marcha de manera posterior al escándalo de *Cambridge Analytica* y *Facebook*, es casi increíble. No obstante, el caso que llevó a Zuckerberg a comparecer ante el Congreso estadounidense fungió como un excelente ejemplo de por qué es necesario regular más estrictamente el manejo de datos. Posiblemente, lo más sorprendente del caso de la compañía *Cambridge Analytica* y su incidencia en la elección presidencial estadounidense, ha sido lo que revela de los datos personales. Su valor económico y de utilidad, así como el potencial que representan no solamente para redes sociales o compañías de marketing pero también para instituciones de seguridad y gobierno no eran evidentes para gran parte de la población. Sin embargo, hoy en día ha quedado claro que nuestros datos tienen un valor y un potencial casi inconmensurable, por lo cual la regulación de la UE parece llegar en el momento indicado.

---

[1] Justin Jaffe, "How Facebook is responding to Europe's new GDPR privacy rules", *CNET*, 11 de abril de 2018. Consultado el 2 de mayo de 2018 en: https://www.cnet.com/how-to/how-facebook-is-responding-to-europes-new-gdpr-privacy-rules/

[2] Marisol Morelos, "Ley de Protección de datos europea aplicará en México*", El Universal,* 17 de febrero de 2018. Consultado el 7 de mayo de 2018 en: http://www.eluniversal.com.mx/techbit/ley-de-proteccion-de-datos-europea-aplicara-en-mexico

[3] *European Data Protection Supervisor*, "Legislation", 2018. Consultado el 4 de mayo de 2018 en: https://edps.europa.eu/data-protection/data-protection/legislation_en

[4] *Ídem*

[5] D*iario Oficial de la Unión Europea,* "Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta el tratamiento de datos personales y a la libre circulación de estos datos por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos)", 27 de abril de 2016. Consultado el 3 de mayo de 2018 en: http://eur-lex.europa.eu/legal-content/ES/TXT/ELI/?eliuri=eli:reg:2016:679:oj

El Reglamento General de Protección de Datos

Aunque dicha regulación fue ratificada en mayo de 2016, la Unión Europea otorgó a toda compañía un periodo de implementación de dos años dentro del cual éstas deberían de adaptar sus modelos y políticas para estar en completo cumplimiento. En las últimas semanas, todas las compañías afectadas por el mismo han estado en contacto con sus usuarios para presentar sus nuevas políticas de privacidad. El documento reemplaza la política de protección de datos aprobada en 1995 y contempla, por ejemplo:

1) Unificar toda regulación de manejo de datos para asegurar un "alto nivel de protección" que sea consistente a través de toda la UE, así como una aplicación de reglas consistente y homogénea.[6] De igual manera, se señala explícitamente que, "la protección otorgada por el presente Reglamento debe aplicarse a las personas físicas independientemente de su nacionalidad o lugar de residencia".

2) Expandir la definición de "datos personales", la cual el órgano Supervisor de Protección define como: "toda información relacionada a una persona identificada o identificable ('sujeto del data'/ *data subject*); una persona identificable es una que pueda ser identificada, directa o indirectamente, en particular por referencia a un número de identificación o más factores específicos sobre su identidad física, fisiológica, mental, económica, cultural o social".[7] Esta definición va más allá de los identificadores obvios como nombre o número de seguridad social, e incluye también, el nombre de usuario utilizado para cuentas de correos electrónicos (ejemplo11@correo.com), así como teléfonos de oficinas, récords médicos y evaluaciones laborales.

3) Establecer claramente las responsabilidades de quienes controlan y procesan los datos, tomando en cuenta la importancia de proveer certidumbre jurídica y transparencia para operadores económicos de distintos tamaños (PyMEs),[8] así como asegurar que las personas físicas de todos los Estados miembros cuenten con "el mismo nivel de derechos y obligaciones exigibles y de responsabilidades para los responsables y encargados del tratamiento". Asimismo, la protección otorgada "debe aplicarse a las personas físicas, independientemente de su nacionalidad o lugar de residencia". De igual manera, el reglamento especifica que no se refiere al "tratamiento de datos de carácter personal por una persona física en el curso de una actividad exclusivamente personal o doméstica", sin relación a actividades profesionales o comerciales, pero sí a quienes proporcionan medios para tratar datos personales dentro de redes sociales.[9]

4) Facilitar el cumplimiento a través del establecimiento de una autoridad supervisora por Estado miembro que funja como garante de la protección de datos y la aplicación de toda

[6] Diario Oficial de la Unión Europea*, op.cit.*
[7] *European Data Protection Supervisor*, "Glossary: P", s.f., consultado el 2 de mayo de 2018 en: https://edps.europa.eu/data-protection/data-protection/glossary/p_en
[8] El reglamento incluye excepciones "en materia de llevanza de registros para organizaciones con menos de 250 empleados" y se específica tomar en cuenta las necesidades de microempresas y empresas pequeñas y medianas.
[9] Diario Oficial de la Unión Europea, *op. cit.*

sanción. Para esto, deberán de existir sanciones equivalentes en todos los Estados así como cooperación continua entre autoridades de control y la Comisión Europea, "sin necesidad de acuerdo alguno entre Estados miembros sobre la prestación de asistencia mutua". Las autoridades de control contarán con las mismas funciones y poderes efectivos, a saber: investigación, poderes correctivos y sancionadores, así como poderes de autorización y consultivos.[10]

5) Exigir que las compañías informen a las autoridades de violaciones de seguridad relativas a sus datos personales, no más de 72 horas después de haber identificado el agravio. La notificación deberá transmitirse también a la autoridad de control competente y deberá abarcar "la naturaleza de la violación […] incluyendo, cuando sea posible, las categorías y el número aproximado de afectados, y las categorías y el número aproximado de registros de datos personales afectados" así como, "describir las posibles consecuencias" y las "medidas adoptadas o propuestas por el responsable para poner remedio a la violación […] incluyendo, si procede, las medidas adoptadas para mitigar posibles efectos negativos". En casos de alto riesgo para los derechos y libertades de las personas físicas, el responsable del manejo de datos deberá informar "sin dilación indebida" a los interesados.[11]

6) Incrementar las penas por violación al reglamento. Se especifica que toda sanción debe ser "adecuada, necesaria y proporcionada", considerando las circunstancias particulares de cada caso. Asimismo, la UE creará un mecanismo de certificación en materia de protección de datos para demostrar el cumplimiento con todo el reglamento, considerando siempre las necesidades de las PyMEs. Entre las penas, se incluye la "limitación temporal o definitiva" del tratamiento de datos, así como multas administrativas, las cuales se aplicarán considerando la naturaleza del/la infractor/a (personas físicas o empresas) estableciento como un máximo, 20 millones de euros o en caso de referirse a una empresa, el 4% del "volumen de negocio total anual global del ejercicio financiero anterior".[12] Asimismo, se considerarán la naturaleza, gravedad y duración de la infracción, las infracciones anteriores, la intencionalidad o negligencia, el grado de cooperación con autoridades de control y las categorías de los datos afectadas por la infracción, entre otras.[13]

[10] *Ídem*
[11] *Ídem*
[12] Cabe destacar que las multas no podrán ser aplicadas retroactivamente, por lo cual no existirán sanciones para las brechas de seguridad ocurridas/descubiertas antes o durante el tiempo de implementación y únicamente los casos ocurridos posterior al 25 de mayo podrán ser considerados bajo las mismas.
[13] *Ídem*

Cambridge Analytica: el valor y el poder de los datos

El caso de la compañía *Cambridge Analytica* (CA) y su relación con *Facebook*, así como la subsecuente comparecencia de Mark Zuckerberg, Presidente de *Facebook*, ante el Congreso estadounidense han esclarecido el creciente valor de los datos personales así como la enorme capacidad para su abuso. Aunque han existido varios ataques y violaciones a la seguridad de *Facebook* así como contra compañías de compras por internet, crédito y otras redes sociales, el caso de CA es destacado dado que los datos personales se utilizaron para enviar mensajes dirigidos a usuarios específicos con la presunta meta de influenciar las elecciones presidenciales de Estados Unidos en 2016. El caso demostró que más allá de simplemente utilizar los datos personales para facilitar compras fraudulentas o fraguar robos de identidad, los datos personales que resguardan las compañías en internet pueden utilizarse para manipular a sus usuarios en beneficio de proyectos políticos o comerciales determinados.

En 2007 en el Centro Psicométrico de la Universidad de Cambridge, los investigadores Michal Kosinksi y David Stillwell, desarrollaron cuestionarios en forma de aplicaciones electrónicas (apps) para *Facebook* que clasificaban a los usuarios dentro de las 5 grandes categorías de personalidad (apertura, consciencia, extroversión, complacencia y neuroticismo) a cambio de lo cual Stillwell y Kosinski tendrían acceso al 40% de los perfiles.[14] Las respuestas de los usuarios revelaban su personalidad y el acceso a sus perfiles permitía a los académicos identificar ciertas correlaciones entre "likes" (me gusta) en *Facebook* y la personalidad del usuario. Por ende, lo que concluyeron fue que era posible predecir la personalidad de millones de personas basados solamente en un cierto número de "likes".[15]

Posteriormente, en 2014, la compañía *Cambridge Analytica*, subsidiaria de SCL Group, (agencia de investigación de mercado para las industrias militares y de defensa) se acercó a Kosinski para utilizar su base de datos, pero las negociaciones no fueron exitosas. No obstante, otro investigador, Aleksandr Kogan, ofreció replicar el modelo de Stillwell y Kosinski ya que él también contaba con autorización para utilizar datos de *Facebook* - con la condición de que éstos fueran utilizados para propósitos académicos. Kogan desarrolló su propio cuestionario y al descargarlo, 320,000 personas permitieron el acceso a la información de su perfil, pero también sin saberlo, a la de sus 'amigos'. No fue sino hasta 2015 que la compañía prohibió el "minado" (como se conoce la recolección de datos) de perfiles de terceros sin su conocimiento.[16]

Gracias a esta información, *Cambridge Analytica* logró crear perfiles "psicográficos" de 30 millones de usuarios y posteriormente desarrolló algoritmos que podían rápidamente perfilar a millones de personas más basados únicamente en algunas características de sus cuentas de *Facebook*.[17] Al tener los perfiles de distintos usuarios identificados, era relativamente simple enviarles mensajes, anuncios o información destinada para persuadirlos de algo, según sus propios sesgos y perfiles psicosociales.

[14] Carole Cadwalladr, "I made Steve Bannon's psychological warfare tool': meet the data war whistelblower", *The Guardian*, 18 de marzo de 2018. Consultado el 2 de mayo de 2018 en: https://www.theguardian.com/news/2018/mar/17/data-war-whistleblower-christopher-wylie-faceook-nix-bannon-trump

[15] *Ídem*

[16] A.S.B., "Why is Mark Zuckerberg testifying before Congress", *The Economist,* 9 de abril de 2018. Consultado el 3 de mayo de 2018 en: https://www.economist.com/blogs/economist-explains/2018/04/economist-explains-7

[17] Robinson Meyer, "The Cambridge Analytica Scandal, in 3 paragraphs", *The Atlantic*, 20 de marzo de 2018. Consultado el 7 de mayo de 2018 en: https://www.theatlantic.com/technology/archive/2018/03/the-cambridge-analytica-scandal-in-three-paragraphs/556046/

Considerando las características de cada usuario, los mensajes podrían ser más sensacionalistas, más académicos, gráficos, explícitos o simples. He aquí la razón por la cual el mal uso de datos en este caso representó un cambio emblemático en la manera que se habla de estos posibles "cibercrímenes". El caso evidenció que los datos personales que tienen compañías privadas sobre nosotros son capaces de ser usados en nuestra contra sin nuestro conocimiento para diversos fines posiblemente nefarios, por actores ajenos a los cual nosotros inicialmente otorgamos nuestra información.

Cabe destacar que este proyecto fue conducido bajo la tutela de Steve Bannon, quién se había interesado en las "operaciones de información" (parte de la doctrina estadounidense de defensa militar que lucha en cinco dimensiones: tierra, mar, aire, espacio e información/ciberespacio)[18] ya que estaba convencido que para cambiar la política debía cambiar la cultura.[19] Su acercamiento en 2013 fue acompañado por financiamiento del multimillonario Robert Mercer con la meta explícita de utilizar la información para diseñar una "ciberguerra electoral".[20] Cabe señalar que el rol de Bannon no fue precisamente secreto dado que fue miembro del Consejo de *Cambridge Analytica*.

En 2016, meses antes de la elección estadounidense, *Facebook* contactó a un ex empleado de *Cambridge Analytica*, Christopher Wylie, para informarle que los datos que habían utilizado habían sido obtenidos ilícitamente y que esta información debía ser destruida inmediatamente. Wylie asegura que la compañía no hizo mucho para asegurar que la información fuera eliminada y que además, "existían múltiples copias" y ésta había sido compartida por medio de correos electrónicos no encriptados.[21] *The Guardian*, uno de los primeros diarios en reportar sobre el *modus operandi* de *Cambridge Analytica* también señaló que existen lazos que atan a la compañía con la campaña de

[18] "Después de la tierra, el mar, el aire y el espacio, la guerra ha llegado a la quinta dimensión: el ciberespacio", proclamó *The Economist* en 2010, luego de que el Presidente Barack Obama declarara que la infraestructura digital del país era un "bien estratégico" para la nación. Ese mismo año el Pentágono estableció su Cyber Comando (*Cybercom*), dirigido por el General Keith Alexander, Director de la Agencia de Seguridad Nacional. La misión del *Cybercom* es defender al ejército estadounidense de ataques, así como desarrollar la capacidad de atacar los sistemas de otros países. Este "quinto elemento" se comenzó a considerar seriamente a finales del siglo XX, pero no fue hasta hace alrededor de diez años que países como China, el Reino Unido, Rusia e Israel comunicaron sus intenciones de "ganar guerras de información" o establecer centros de ciberseguridad. En 1995, el General Ronald R. Fogleman, Jefe del Gabinete de la Fuerza Aérea, aseguró en un discurso en Washington D.C. que, la "explosión de información" implicaba una nueva frontera y que "dominar en el ámbito de la información sería crítico para el éxito militar futuro". Con información de: *The Economist,* "War in the fifth comain", 1 de julio de 2010; y, Gen. Ronald R. Fogleman, "Information Operations: The Fifth Dimension of Warfare", *Information Warfare Site*, 25 de abril de 1995. Ambos consultados el 9 de mayo de 2018 en: https://www.economist.com/node/16478792 y http://www.iwar.org.uk/iwar/resources/5th-dimension/iw.htm

[19] El concepto, para Bannon, está alineado con las ideas de Andrew Breitbart, fundador de *Breitbart News.* Breitbart creó el portal con la meta de "impulsar una guerra" en contra de lo que él consideraba era "el complejo mediático demócrata". El fundador consideraba que el cine, la televisión y la música popular eran vehículos para la difusión de mensajes políticos los cuales se repetían múltiples veces a través del día y que estos respondían a una hegemonía liberal. Breitbart aseguraba que éstos, "dan forma a la cultura, y la cultura da forma a la política" por ende, su teoría era que si podía influenciar dichos espacios culturales podría influenciar la política para asemejarse más a su visión conservadora. Su estrategia era la de constante conflicto, la creación de una "guerra cultural" en la cual el movimiento conservador ya no estaría representado por "sumisos de corbata de moño", aseguró Kurt Schlichter, cercano al fundador del sitio. No obstante, muchos consideran que desde sus inicios Breitbart tuvo una índole explícitamente política y no tanto cultural. Breitbart insistía en representar a los conservadores estadounidenses como una minoría amenazada por un "Marxismo cultural" de la izquierda que era "moralmente equívoco" y peligrosa. Tras el fallecimiento de su fundador en 2012, Steve Bannon tomó control de la organización y su enfoque fue aún más político. Cuando Trump anunció su candidatura, Bannon consideró que sería ideal para derrotar a las "élites globales" y utilizó el sitio para impulsar su proyecto hacia la Casa Blanca. Con información de: Jane Coaston, "Bannon's Breitbart is dead. But Breitbart will live on", *Vox*, 14 de enero de 2018; y, Conor Friersdorf, "Breitbart.com struggles with the contradictions of its namesake", *The Atlantic*, 1 de noviembre de 2012. Ambos consultados el 9 de mayo de 2018 en: https://www.vox.com/2018/1/14/16875288/bannon-breitbart-conservative-media y https://www.theatlantic.com/politics/archive/2012/11/breitbartcom-struggles-with-the-contradictions-of-its-namesake/264372/

[20] Carole Cadwalladr, *op. cit.*

[21] Carole Cadwalladr, *op. cit.*

Brexit. Wylie ha admitido que él participó activamente en la creación de *AggregateIQ* (AIQ), la cual recibió alrededor del 40% del presupuesto de la campaña en contra de permanecer en la UE, *Vote Leave*.[22] Asimismo, *Cambridge Analytica* también otorgó sus servicios a la campaña liderada por el euroescéptico Nigel Farage, *Leave.EU*.[23] Aunque no existe evidencia de que el mismo mal uso de datos ocurrió en el caso británico, Wylie testificó ante el Parlamento británico a finales de marzo y aseguró que AIQ utilizaba la base de datos de *Cambridge Analytica*.[24]

En total, en el Reino Unido se reportaron casi tres millones y medio de libras destinadas *a Cambridge Analytica* o AIQ mientras que en Estados Unidos, la compañía recibió casi 20 millones de dólares entre 2015 y 2016, la mayoría de grupos conservadores a favor de candidatos republicanos.[25] Sin embargo, aunque éstas elecciones han sido las más mencionadas en el caso de *Cambridge Analytica*, la compañía, por medio de SCL, ha participado en más de 100 campañas electorales, incluyendo elecciones presidenciales o de Primeros Ministros en: Kenia, 2017; Nigeria, 2015; India, 2014; entre otras.[26] Asimismo, en 2017 se hizo público que estaba recolectando información de ciudadanos mexicanos y colombianos a través de una app llamada *Pig.gi* que pagaba a sus usuarios por ver comerciales y completar encuestas.[27] Aunque *Cambridge Analytica* negó trabajar para algún partido político en México, *Bloomberg* reportó que la empresa había sido, de hecho, abordada por varios partidos.

[22] Carole Cadwalladr, Mark Townsend, "Revealed: the ties that bound Vote Leave's data firm to controversial Cambridge Analytica", *The Guardian*, 24 de marzo de 2018. Consultado el 4 de mayo de 2018 en: https://www.theguardian.com/uk-news/2018/mar/24/aggregateiq-data-firm-link-raises-leave-group-questionshttps://www.theguardian.com/uk-news/2018/mar/24/aggregateiq-data-firm-link-raises-leave-group-questions.

[23] Carole Cadwalladr, Mark Townsend, *op. cit.*

[24] David Martin, "What role did Cambridge Analytica play in the Brexit vote?", *DW,* 27 de marzo de 2018. Consultado el 2 de mayo de 2018 en: http://www.dw.com/en/what-role-did-cambridge-analytica-play-in-the-brexit-vote/a-43151460

[25] David Martin, op. cit; y, Maegan Vazquez, "Trump isn't the only Republican who gave Cambridge Analytica big bucks", *CNN,* 21 de marzo de 2018. Consultado el 3 de mayo de 2018 en: https://edition.cnn.com/2018/03/20/politics/cambridge-analytica-republican-ties/index.html

[26] *BBC,* "Cambridge Analytica: the data firm's global influence", 22 de marzo de 2018. Consultado el 4 de mayo de 2018 en: http://www.bbc.com/news/world-43476762

[27] Nacha Cattan, "Trump's big-data guru scouts presidential candidates in Mexico", *Bloomberg*, julio 19 de 2017. Consultado el 3 de mayo de 2018 en:https://www.bloomberg.com/news/articles/2018-05-07/fox-jumps-on-report-that-comcast-is-mulling-counterbid-to-disney

Zuckerberg ante el Congreso estadounidense

Dado que el caso de *Cambridge Analytica* afectó a millones de ciudadanos estadounidenses y presumiblemente jugó un papel importante en la elección presidencial de 2016, el Congreso pidió a Mark Zuckerberg, CEO de *Facebook* presentarse a testificar el 10 y 11 de abril. Aunque previamente Zuckerberg había sido convocado por anteriores violaciones a la seguridad de los datos de sus usuarios, esta fue la primera vez que el líder de la compañía decidió asistir y no mandar representantes. El CEO se presentó ante las Comités de Comercio y de Asuntos Legales del Senado el 10 de abril, el primer día de dos largas comparecencias que duraron un total de casi diez horas. Mucha de la información que se dio a conocer durante estas dos sesiones es de gran interés. No obstante, cabe destacar que lo que esta audiencia reveló del modelo de negocios de *Facebook* así como de su capacidad para rastrear y guardar información de sus usuarios son elementos de particular importancia.

Desafortunadamente, la comparecencia no fue aprovechada como quizás pudo haber sido por los legisladores presentes, dado que un gran número de preguntas revelaron una falta de conocimiento básico de la operación de *Facebook*, su modelo de negocios y hasta el funcionamiento del internet. Destaca por ejemplo, que el Senador Orrin Hatch (R-Utah), preguntó de qué manera planeaba continuar operando la plataforma de manera gratuita, a lo cual Zuckerberg contestó simplemente que "vendían anuncios" – justamente el mecanismo que ese día los convocaba.[28]

No obstante, la aparente ingenuidad de su pregunta resaltó un tema crucial: el hecho que para que las plataformas permanezcan "gratuitas" para los usuarios, éstas deben de extraerle valor a los mismos de alguna u otra forma. En otras palabras, "si no estás comprando el producto, tú eres el producto".[29] *Facebook* no ha basado su modelo de negocios alrededor de la idea de "vender" datos personales pero sí alrededor de recolectar información de sus dos mil millones de usuarios a nivel mundial para después vender acceso a los mismos.[30] Hoy en día el 98% de las ganancias de la compañía provienen de venta de publicidad; esencialmente lo que *Facebook* hace es resguardar la información de sus usuarios – de venderla a cualquier compañía ésta perdería valor.[31] Las empresas que desean tener anuncios en *Facebook* compran acceso a ciertos sectores, por ejemplo, mujeres de 30 años que están interesadas en seguros de vida, o estudiantes de licenciatura que vivan en Guadalajara, Jalisco.[32]

La información agregada de *Facebook* hace posible que la compañía ponga anuncios perfectamente dirigidos: por eso, cuando buscamos en *Google*, "zapatos negros", posteriormente los *banners*[33] que aparecen en la plataforma y nos anuncian exactamente eso. Esto también tiene que ver con algo que

[28] Bloomberg Government, "Transcript of Mark Zuckerberg's Senate hearing", *The Washington Post*, 10 de abril de 2018. Consultado el 7 de mayo de 2018 en: https://www.washingtonpost.com/news/the-switch/wp/2018/04/10/transcript-of-mark-zuckerbergs-senate-hearing/?utm_term=.8edb7bea1009
[29] Matthew Rosenberg, Gabriel J.X. Dance, "You're the product", *New York Times,* 8 de abril de 2018. Consultado el 2 de mayo de 2018 en: https://www.nytimes.com/2018/04/08/us/facebook-users-data-harvested-cambridge-analytica.html
[30] Kurt Wagner, "This is how Facebook uses your data for ad targeting", *Recode*, 11 de abril de 2018. Consultado el 7 de mayo de 2018 en: https://www.recode.net/2018/4/11/17177842/facebook-advertising-ads-explained-mark-zuckerberg
[31] Reuters, "Facebook now has an almost advertising-only business model" *Fortune*, 5 de mayo de 2017. Consultado el 7 de mayo de 2018 en: http://fortune.com/2017/05/05/facebook-digital-advertising-business-model/
[32] Kurt Wagner, *op. cit.*
[33] Anuncios en páginas de internet, generalmente están de los lados o en la parte superior.

admitió Zuckerberg durante sus comparecencias, que la compañía sí tiene mecanismos para rastrear la actividad en internet de sus usuarios, aun cuando éstos han cerrado *Facebook*.[34] Esto se logra a través de *cookies* (galletas), que son esencialmente un pixel enviado por parte del sitio web que permanece dentro de la pantalla del usuario, siguiendo sus movimientos sin que éste se entere. Hoy en día, un gran número de sitios usa estas "galletas" y aunque también avisan al usuario previo al acceso a la página, ocurre lo mismo que con las políticas de *Facebook*: la población en general no entiende el concepto ni las implicaciones que éstas podrían tener a largo o mediano plazo. Asimismo, Zuckerberg reveló "no saber" por cuánto tiempo se conserva la información de usuarios que han cerrado sus cuentas en la plataforma (o en *Instagram*, aplicación dedicada a la fotografía que fue comprada por *Facebook* en 2012), pero aseguró que intentan borrar la información "lo más rápido posible".[35]

El CEO insistió a través de su comparecencia que su compañía es transparente y sí permite a sus usuarios no otorgar datos personales a terceros, además de que señaló en repetidas ocasiones que cada aplicación que cualquier usuario decida ligar a *Facebook* (por ejemplo, Uber, plataformas de juegos, etc.) presenta sus términos y condiciones y requiere de la aprobación del interesado. Asimismo, reiteró que su compañía siempre ha sido "idealista y optimista" y que su meta ha sido conectar a las personas a través de una plataforma que puede amplificar sus voces, así como crear comunidades e impulsar negocios.[36]

Consideraciones finales

Michal Kosinski, el psicólogo de la Universidad de Cambridge que guio las primeras investigaciones acerca de cómo nuestra huella digital en internet puede ser usada para identificar preferencias, personalidades y actitudes, considera que *Cambridge Analytica* no es tema de preocupación; en particular "comparado con lo que pueden hacer los gobiernos o las compañías más serias".[37] Kosinski asegura que la campaña de 2008 de Obama fue pionera en los mecanismos de "*micro-targetting* psicológico" (identificar perfiles psicológicos para tener mayor éxito persuasivo) y que hoy en día, los gobiernos siguen a los ciudadanos en internet para distinguir entre actitudes benignas y posibles amenazas. Kosinski también ha asegurado que en el futuro no tan distante, la privacidad es un concepto casi inexistente.[38] Lo anterior, no necesariamente en términos de que estemos bajo constante vigilancia (aunque definitivamente nuestra dependencia de aparatos móviles facilita la misma), pero dado que la información que hemos ya compartido, canalizada a máquinas de inteligencia artificial, es capaz de predecir muchos de nuestros comportamientos.

Es importante reflexionar sobre en qué medida nuestra dependencia a servicios "gratuitos" se ha extendido a todas las áreas de nuestra vida. Indudablemente, existe el riesgo de que las plataformas digitales que utilizamos para socializar, conseguir trabajo, mantenernos informados, comunicarnos con nuestros seres queridos, compartir información, planear viajes y consumir entretenimiento lucren

[34] Bloomberg Government, "Transcript of Mark Zuckerberg's Senate hearing", *op. cit.*
[35] *Ídem*
[36] *Ídem*
[37] John Morgan, "Michal Kosinski: enemy of privacy or just a whistleblower?" Times Higher Education, 22 de marzo de 2018. Consultado el 7 de mayo de 2018 en: https://www.timeshighereducation.com/features/michal-kosinski-enemy-privacy-or-just-whistleblower#survey-answer
[38] *Ídem*

con nuestros datos. Éstos podrían escapar a nuestro control, y cada día se vuelve más difícil pensar en optar por no participar en dichos sistemas. En efecto, una pregunta constante en la comparecencia de Zuckerberg fue qué opciones tienen las personas que no estén de acuerdo con sus políticas; resulta evidente que no hay alternativas, los monopolios cibernéticos son globales y prácticamente ineludibles, al menos para millones de personas.[39]

No obstante, es una buena noticia que las nuevas sanciones, al menos las contempladas en el espacio europeo, incorporen multas mucho más altas que las previamente consideradas. Hoy en día (previo a la entrada en vigor del nuevo RGPD) éstas ascienden a un máximo de setecientos mil euros, mientras que bajo el nuevo modelo la multa máxima podría ascender al 4% de las ganancias globales del año anterior. Para una compañía como *Google*, en 2016 esto hubiera implicado una multa de 3.5 mil millones de dólares ya que el año anterior reportó ganancias de 89 mil millones de dólares; mientras que para *Facebook*, la máxima multa aplicada en 2017 sería de 400 millones de dólares dado que en 2016 reportó 10 mil millones de dólares de ganancias.[40] Asimismo, la amenaza de suspender la capacidad de recolectar datos no es una consideración menor. Solamente la aplicación de estas leyes y la realidad de la puesta en práctica de las mismas nos revelarán si son suficientes para cambiar los comportamientos de ciertas compañías.

Sin embargo, seguramente lo más importante de las sanciones y los protocolos de manejo de datos, es que por más que éstos no sean perfectos, son el primer paso en términos de admitir y tratar de regular aspectos de la realidad actual. Los datos de millones de personas sí están siendo compartidos para usos indebidos y casi siempre no autorizados. Conformarse simplemente con que cualquier compañía puede abusar de ello solamente limitada por una presunta autocensura, no es de ninguna manera un modelo sostenible. Hasta ahora, no hay forma de saber si el posible castigo será suficiente para hacer que las compañías actúen de manera más disciplinada. No obstante, está en el mayor interés de los gobiernos, continuar informándose sobre dichas políticas, así como de la manera en la cual funcionan las aplicaciones para poder tomar decisiones más informadas y reclamar el respeto a nuestros derechos cuando el caso lo amerite.

[39] Bloomberg Government, “Transcript of Mark Zuckerberg’s appearance before House committee”, *op. cit.*
[40] *Statista*, “Google revenue worldwide from 2002 to 2017 (in billions U.S. dollars)”, 2018; y “Facebook’s annual revenue and net income from 2007 to 2017 (in million U.S. dollars)”, 2018. Ambos consultados el 4 de mayo de 2018 en: https://www.statista.com/statistics/266206/googles-annual-global-revenue/#0 y https://www.statista.com/statistics/277229/facebooks-annual-revenue-and-net-income/

CENTRO DE ESTUDIOS INTERNACIONALES
GILBERTO BOSQUES
ANÁLISIS E INVESTIGACIÓN

Coordinadora General
Adriana González Carrillo

Coordinación y revisión
Arturo Magaña Duplancher
Ana Margarita Martínez Mendoza

Investigación y elaboración
Inés Carrasco Scherer

Mayo de 2018

El **Centro de Estudios Internacionales Gilberto Bosques** del Senado de la República tiene como objeto la realización de estudios y el acopio de información sobre temas de política internacional y política exterior de México; así como el prestar apoyo a las comisiones de relaciones exteriores para el desarrollo de sus actividades y el ejercicio de las facultades exclusivas del Senado en materia de política exterior; además de auxiliar a los órganos directivos, comisiones, grupos parlamentarios y senadores que así lo requieran en cuanto a diplomacia parlamentaria y protocolo en el ámbito internacional.

CGBSenado

http://centrogilbertobosques.senado.gob.mx/

Referencia para citar este documento:
Centro de Estudios Internacionales Gilberto Bosques, "El impacto global de la regulación europea en materia de datos personales ", Nota de Coyuntura, México, *Senado de la República*, 10 de mayo de 2018.