UNA VOTACIÓN MUY SECRETA

Lucy Purdon

• *Un estudio de caso* •
sobre el proceso electoral en Kenia

RESUMEN

Este artículo se centra en las elecciones en Kenia y analiza el uso de la tecnología y la explotación de los datos personales tanto en el proceso electoral como en la campaña. Solo tenemos que ver la historia electoral de Kenia para entender por qué esto es importante. Las elecciones de 2007/2008 resultaron en una violencia que mató a 1000 personas y desplazó a más de 600,000. Las elecciones de 2013 fueron relativamente pacíficas, pero estuvieron marcadas por el aumento de "expresiones de odio" en internet que explotaron las tensiones étnicas. El resultado de las elecciones de 2017 fue anulado y repetido en medio de una gran tensión, con al menos 33 personas muertas, y hubo una publicidad política personalizada en internet que manipuló el miedo que había en el país de que hubiese más violencia. Este artículo concluye con un esbozo de las protecciones y garantías mínimas, que puede aplicarse mundialmente.

PALABRAS CLAVE

Kenia | Elecciones | Votar | Políticas | Biometría | Tecnología | Datos | Elaboración de perfiles | Propaganda | Campañas electorales | Piratería informática (Hacking) | Seguridad | Bases de datos | Desinformación | Protección de datos | Análisis de datos

2018 es un año con muchos procesos electorales: Brasil, Colombia, México, Paquistán, Zimbabue y al parecer Tailandia van a celebrar elecciones generales o presidenciales. La seguridad y transparencia de los procesos electorales está siendo examinada globalmente. Desde la adopción apresurada del registro biométrico de los electores, las preocupaciones sobre la seguridad de los registros de votantes y de los propios sistemas de votación, hasta el fenómeno de publicidad política personalizada y campañas de desinformación en los medios sociales, hay muchas cosas para distraer a los votantes de la pregunta más importante para la democracia, ¿quién te representará mejor a ti y a tu país?

Este artículo se centra en las elecciones en Kenia y analiza el uso de la tecnología y la explotación de los datos personales tanto en el proceso electoral como en las campañas.

Solo tenemos que ver la historia electoral de Kenia para entender por qué esto es importante. Las elecciones de 2007/2008 resultaron en una violencia que mató a 1000 personas y desplazó a más de 600,000. Las elecciones de 2013 fueron relativamente pacíficas, pero estuvieron marcadas por el aumento de "expresiones de odio" en internet que explotaron las tensiones étnicas. El resultado de las elecciones de 2017 fue anulado y repetido en medio de una gran tensión, con al menos 33 personas muertas, y hubo una publicidad política personalizada en internet que manipuló del miedo que había en el país de que hubiese más violencia.

Este artículo está basado en una investigación de *Privacy International* durante las elecciones presidenciales de 2017 sobre los orígenes de dos controvertidas campañas en internet y la participación de dos empresas de análisis de datos occidentales.[1] Este artículo también recurre a investigaciones publicadas por el Centro de Propiedad Intelectual y Tecnología de la Información (CIPIT, por su sigla en inglés) de la Universidad de Strathmore en Kenia, en colaboración con *Privacy International,* analizando la adopción e implementación del registro biométrico de votantes.[2] Además, este artículo refleja el trabajo de incidencia política y desarrollo de políticas que emprendió *Privacy International* tras el escándalo Facebook/*Cambridge Analytica* que salió a la luz en marzo de 2018 y que también puso el foco en las elecciones de 2017 en Kenia.

1 • El registro biométrico de votantes

Cuando el gobierno de Kenia anunció la adopción del registro y autenticación biométricos de votantes (BVR, por su sigla en inglés) en la Ley de Elecciones de 2011, las motivaciones eran razonables. La recomendación de pasar a un sistema de registro nuevo fue hecha por la Comisión Kriegler, que fue creada para investigar el sistema electoral de Kenia tras la violencia post electoral de 2007/2008.[3] El informe de la Comisión Kriegler también proporcionó una nota técnica sobre las características de los sistemas biométricos de votación.[4]

Se pensaba que un sistema BVR, incluyendo las huellas digitales de los votantes, además de la verificación en el colegio electoral, garantizaría una persona por voto y evitaría acusaciones de irregularidades en la urna electoral. Los resultados podrían ser transmitidos directamente

al cuerpo electoral, evitando cualquier posible manipulación. Había sospechas de que había votos que estaban siendo emitidos en nombre de personas fallecidas que todavía estaban en el registro de votantes. La Comisión Kriegler estimó que "probablemente" había 1,2 millones de personas fallecidas en el registro de 2007,[5] pero no había cifras disponibles para corroborar la sospecha de que se estaban emitiendo votos en su nombre en esas elecciones o en elecciones posteriores. Esta preocupación fue repetida por George Morara, presidente de la Comisión Nacional de Derechos Humanos de Kenia (KNCHR, por su sigla en inglés) al decir antes de las elecciones de 2017 que "en Kenia, la gente dice que los muertos vuelven para votar y después regresan a sus tumbas."[6] ¿Pero había alguna solución alternativa, menos costosa e intrusiva, que un BVR? ¿No podría haber solucionado el problema una reforma del registro de nacimientos y fallecimientos? Esto nunca se debatió.

Antes de embarcarse en iniciativas potencialmente intrusivas con enormes cantidades de datos, los gobiernos deberían preguntarse, ¿para qué hacer todo esto? ¿Qué problema pretende solucionar, por ejemplo, una base de datos biométricos? ¿Cómo lo logrará? ¿Cuáles son las consecuencias si fracasa?

Una de las preocupaciones principales es que los gobiernos están muy dispuestos a implementar iniciativas que recogen grandes cantidades de datos personales, pero no se preocupan tanto de garantizar los datos personales que esos proyectos generan. Los sistemas biométricos son un ejemplo de sistemas con gran cantidad de datos que son potencialmente muy intrusivos. La preocupación de los defensores de derechos humanos de Sudáfrica, por ejemplo, es que cuando se adoptan estos sistemas sin que hayan marcos jurídicos sólidos y garantías estrictas, las tecnologías biométricas representan graves amenazas a la privacidad y la seguridad personal, pues su aplicación puede ser ampliada para favorecer la discriminación, la elaboración de perfiles y la vigilancia masiva.[7] Otra preocupación es que las variaciones en la precisión y en la tasa de fallos de la tecnología pueden conducir a identificaciones erróneas, al fraude y a la exclusión civil, un factor central en los constantes desafíos con los que está lidiando actualmente la Corte Suprema de la India en relación al esquema biométrico Aadhaar, actualmente empleado en la India.[8]

En el caso de Kenia, la tecnología tuvo fallos enormes durante las elecciones de 2013, y los colegios electorales tuvieron que recurrir al registro manual para identificar a los votantes. En 2017, el sistema funcionó relativamente bien comprado a la debacle de 2013,[9] pero como analiza este artículo, el grado en el que la tecnología biométrica ha mejorado la credibilidad de la democracia y las elecciones en Kenia es todavía un tema controvertido, debido a diversos otros factores.

2 • La seguridad de la bases de datos de los votantes

Las bases de datos de registro de votantes están a menudo poco protegidas y son vulnerables. Hay filtraciones de datos por todo el mundo, y las cantidades involucradas

están en aumento. La información personal de más de 93 millones de votantes en México,[10] incluyendo sus domicilios, fueron publicados abiertamente en internet después de ser tomados de una base de datos gubernamental poco protegida. Esto puede ser una información sumamente delicada dado el contexto; en México por ejemplo se calcula de cada año son secuestradas hasta 100,000 personas.[11] Del mismo modo, la información personal de más de 55 millones de votantes filipinos fue puesta en internet a disposición del público, la mayor filtración de datos en la historia de Filipinas.[12]

Las investigaciones llevadas a cabo en Kenia para descubrir si la base de datos de votantes de 2017 fue compartida con terceros, y si lo fue con quién, mostraron que el registro estaba públicamente disponible a la venta, sin protecciones ni garantías. En consecuencia, los votantes recibieron mensajes de texto no solicitados de los candidatos, identificando al receptor con su nombre, circunscripción e incluso colegio electoral.[13] Ya podemos ver que estas aplicaciones tecnológicas están lejos de devolver la tan necesitada confianza.

3 • El problema con la falta de protección de los datos

Kenia no tiene una legislación exhaustiva sobre protección de datos que obligue a una entidad, pública o privada, a respetar las normas fundamentales de protección de datos. Esto incluiría detallar lo que es recogido, el objetivo de la recolección, cómo se va a almacenar y con quién será compartido. En la nueva legislación de protección de datos en Europa por ejemplo, las entidades deben proporcionar el fundamento jurídico para la recolección y obtener el consentimiento informado del individuo, en particular para el procesamiento de datos personales delicados, como los datos biométricos. Sin leyes adecuadas de protección de datos, los individuos quedan vulnerables a que se recoja una cantidad excesiva de datos sobre ellos, sin su consentimiento y que se utilicen de maneras que no conocen. Cuando las empresas recogen datos en países con una legislación insuficiente y la comparten con terceros, no está claro que normas ellos, y estos terceros, están siguiendo, si es que alguna. Donde se generan los datos, los individuos deberían poder descubrir qué organizaciones y empresas tienen qué tipos de datos sobre ellos y para qué los utilizan. Tener una ley en los libros es una cosa bien distinta a tener una ley implementada eficazmente. Un elemento fundamental es una autoridad independiente que disponga de recursos adecuados y sea capaz de investigar las reclamaciones.

¿La protección de datos habría ayudado en las situaciones esbozadas en este artículo? Podría haber llevado al gobierno de Kenia a pensárselo dos veces antes de implementar el sistema en la manera en que lo hicieron. Habría hecho más fácil para los keniatas ejercer sus derechos y obtener respuestas sobre, por ejemplo, el tipo de datos que estaban siendo recogidos, cómo se estaban utilizando, cuánto tiempo se almacenaban, y con quién eran compartidos.

Las dos secciones siguientes analizan el tema en un contexto diferente.

4 • Desinformación y propaganda

En países de todo el mundo, la difusión de desinformación y propaganda durante época electoral ha sido un problema durante décadas, sin embargo ha recibido poca atención e interés internacional. Resulta frustrante que, cuando recientemente se convirtió en un problema en los Estados Unidos de América (EE.UU) durante las elecciones presidenciales de 2016 y también en Europa en relación al Brexit, de repente adquirió un nombre: "noticias falsas".[14]

La segunda década del siglo XXI ha visto como los medios sociales eran aclamados por provocar revoluciones y cambios democráticos.[15] Se prestó menos atención a las tensiones políticas y sociales amplificadas en esos mismos espacios. Silicon Valley no logró predecir, comprender, ni siquiera tratar de entender lo que estaba ocurriendo en el mundo, ni escuchó las repetidos avisos de que el contenido concebido para avivar tensiones étnicas publicado en sus plataformas tenía efectos en el mundo real. En Kenia por ejemplo, ya se sabía que los mensajes de texto, los blogs y la radio había desempeñado un papel en la violencia post electoral de las elecciones 2007/2008.[16] Las elecciones de 2013 también estaban plagadas de contenido polémico e incendiario en los medios sociales, donde encontraron salida tras haberse establecido controles más rigurosos en los medios impresos y las telecomunicaciones.[17]

El espacio en línea es un imán de todo durante la época electoral. Las campañas políticas siempre han sido un asunto turbio y aunque las campañas políticas basadas en datos no son nuevas, la escala de los datos disponibles y el poder potencial de influenciar o reprimir a los votantes con esos datos sí lo es, sobre todo mediante los anuncios políticos personalizados en internet.

5 • Anuncios políticos personalizados basados en análisis de datos

Las campañas políticas de todo el mundo se han convertido rápidamente en sofisticadas operaciones de datos. El modo en que los datos son utilizados en elecciones y campañas políticas es potencialmente muy invasivo de la privacidad, plantea interrogantes importantes sobre la seguridad y tiene el potencial de socavar la confianza en el proceso democrático.

Las plataformas de los medios sociales ganan dinero con los anuncios personalizados, basados en la información del usuario que recogen, incluyendo información demográfica, localización e intereses detallados.[18] Del mismo modo en que la publicidad en línea escoge a sus destinatarios basándose en los intereses, personalidad y estado de ánimo para vender sus productos, los partidos políticos te persuaden a que compres lo que venden cuando llega la época de elecciones.

En resumen, esto quiere decir que hay empresas, muchas de las cuales probablemente no conozcas su nombre, que son capaces de conocer tus hábitos, personalidad, intereses sexuales, creencias políticas y más cosas para hacer predicciones sobre tu personalidad

y comportamiento. Esto se conoce como "elaboración de perfiles".[19] La elaboración de perfiles genera inferencias y predicciones muy sofisticadas sobre la personalidad, comportamiento y creencias de la persona. En definitiva, se están elaborando perfiles de los votantes basados en información que ellos no sabían necesariamente que estaban proporcionando. Esto es particularmente preocupante cuando información delicada, como creencias políticas y rasgos de personalidad son inferidos a partir de datos que no guardan ninguna relación con esas cuestiones, utilizando la elaboración de perfiles.

Los partidos políticos participando de las elecciones contratan directamente empresas de análisis de datos y medios digitales, que son expertos en la elaboración de perfiles, para dirigir sus campañas en internet. Estas empresas, a su vez, puede que trabajen directamente con plataformas en línea, como Facebook, para crear mensajes políticos personalizados con el fin de influenciar tu voto, basándose en información recogida e inferida sobre ti. Con frecuencia se basan en datos disponibles comercialmente de proveedores de datos, o registros y datos disponibles públicamente en internet para elaborar perfiles muy íntimos, incluyendo conclusiones sobre tu personalidad, miedos y estado emocional. Después se puede hacer que los mensajes y anuncios personalizados de las campañas inunden los resultados de los buscadores y las fuentes de los medios sociales. La campaña presidencial de Trump de 2016, por ejemplo, utilizó de 40 a 50,000 variaciones de los mismos mensajes en internet cada día para llegar a distintos grupos de personas.[20] Pero los detalles detrás de estos procesos con frecuencia no están claros; exactamente para quién trabajan estas empresas, qué hacen, cómo lo hacen, que datos recogen y cuánto éxito tienen, son secretos muy bien guardados.

A comienzos de 2017, *Privacy International* investigó un informe que la empresa de análisis de datos *Cambridge Analytica*, con sede en el Reino Unido, estaba haciendo para el partido gobernante *Jubilee*, durante la campaña de las elecciones presidenciales de Kenia. Escribimos a la empresa en mayo de 2017 pidiendo una clarificación sobre cuál era su papel y cómo, siendo una empresa británica, estaba cumpliendo las leyes de protección de datos siendo el caso que Kenia no tiene ninguna.[21] Estábamos preocupados por el hecho de que la potencial recopilación de datos podría ser extremadamente intrusiva, incluyendo datos personales delicados, tales como la etnia de las personas. En países donde hay una historia de tensiones étnicas que resultan en violencia política, como en Kenia, las campañas basadas en análisis de datos y elaboración de perfiles es un terreno sin explorar, plagado de riesgos. No recibimos ninguna respuesta.

Nuestras fuentes confirmaron que *Cambridge Analytica* estaba trabajando para el partido *Jubilee*, recopilando datos de encuestas para proporcionar asistencia en la campaña y gestionar la imagen del presidente. Por esas mismas fechas, dos campañas incendiarias en internet, *The Real Raila* y *Uhuru For Us*, dirigidas contra la oposición keniata comenzaron a difundirse por internet en Kenia. Su creación fue reivindicada por "un grupo variado y preocupado de jóvenes keniatas", y jugó mucho con las elecciones pasadas de Kenia y los miedos de más violencia en el futuro. La campaña *The Real Raila* proclamaba que la administración del candidato de la oposición Raila Odinga "eliminaría a tribus enteras".[22]

Como estos videos dominaban las búsquedas de Google e inundaban las cuentas de Twitter, Facebook y YouTube por todo el país durante 2017, *Privacy International* llevó a cabo una investigación en profundidad[23] sobre la procedencia de los videos.

Como ya se había demostrado que *Cambridge Analytica* estaba trabajando para el partido *Jubilee*, suponíamos que la empresa había participado en algún grado en la creación de los videos. Sin embargo, la investigación de *Privacy International* mostró que Harris Media LLC creó los videos, una agencia con sede en Texas que usa análisis de datos para crear campañas políticas. En esta ocasión, la personalización fue llevada a cabo mediante el uso juicioso de Google AdWords, donde anuncios pagados para las campañas aparecían encima de los resultados de Google para muchos términos relacionados a las elecciones de Kenia, tales como "fecha de las elecciones en Kenia".

No obstante, fue solo en marzo de 2018, tras las investigaciones del periódico *The Guardian* y *Channel 4 News* en el Reino Unido que *Cambridge Analytica* fue lanzada a las primeras páginas de las noticias. Una persona denunció lo que describió como "cosecha" de perfiles de Facebook para dirigir mensajes personalizados a los votantes durante las elecciones presidenciales de EE.UU. de 2016.[24] Una investigación encubierta de *Channel 4 News* grabó con cámara oculta a empleados de *Cambridge Analytica* alardeando de su implicación en distintas elecciones, incluyendo en Kenia. Mark Turnbull, el director general de *Cambridge Analytica Political*, una filial de *Cambridge Analytica*, confirmó esto y más cosas en un video grabado con cámara oculta,

> *Hemos cambiado el nombre del partido dos veces, escrito su manifiesto, hecho dos rondas de 50,000 encuestas, una enorme cantidad de investigación, análisis, enviado mensajes y después escrito todos los discursos y lo hemos preparado todo, así que prácticamente todos los elementos de su campaña.*[25]

Posteriores informaciones de *Channel 4 News* enfocadas en Kenia también señalaron la difusión de videos en internet[26] detallada en nuestra investigación anterior. Lo que seguimos sin saber, no obstante, es qué tipo de datos de los ciudadanos keniatas fueron recopilados, de qué fuentes y cuál fue exactamente la participación de *Cambridge Analytica*. No sabemos, por ejemplo, qué datos pueden haber sido recogidos o compartidos, sea por Facebook, otras plataformas, u otras empresas de análisis de datos trabajando en Kenia durante las elecciones.[27]

Sin embargo, el escándalo generó una positiva oleada de análisis y discusión sobre el comportamiento de las corporaciones y la falta de garantías para los datos personales en toda África.[28] Esta historia que todavía se está desarrollando muestra un ecosistema corporativo poderoso y opaco detrás de la publicidad política personalizada en internet que se alimenta de nuestros datos personales; ya sea para vendernos jabón o para convencernos de a quién votar.

6 • Transparencia en las campañas políticas

En países con una historia de violencia política, no debería ignorarse este hecho. La etnicidad en Kenia, por ejemplo, es todavía un tema delicado y las elecciones son un momento en que la tensión se intensifica. Por tanto, como mínimo, las empresas en este ecosistema deben ser transparentes sobre su papel en las campañas políticas en internet. Las leyes electorales de Kenia no exigen claramente que los candidatos respondan por las campañas y anuncios que han financiado. Las empresas involucradas no son claras sobre su papel que están desempeñando. Es esencial que las campañas políticas se desarrollen de un modo transparente y responsable, sobre todo cuando hay tanto en juego en un país como Kenia. Actualmente los anuncios políticos personalizados en internet no son ni una cosa ni la otra.

No es controvertido exigir a los partidos políticos que sean transparentes sobre las campañas publicitarias que han financiado, el modo como han desarrollado los mensajes personalizados, o con qué empresas han trabajado. Cuando no hay transparencia sobre quién ha financiado o creado los anuncios de campaña, no hay rendición de cuentas.

Una democracia saludable no consiste únicamente en votar. Kenia es solo uno de los países donde el registro y autentificación biométrica de los votantes presenta desafíos, y va a llevar tiempo desentrañar la maraña de empresas explotando los datos personales para campañas pagadas por partidos políticos. La dificultad, por supuesto, es que los que se benefician son los propios partidos políticos. ¿Por qué cambiar un sistema que los ayuda a obtener el poder? Los keniatas deben esperar unos años para las próximas elecciones. Para todos aquellos que tienen elecciones este año, protegedlas exigiendo transparencia y protecciones adecuadas, desde el registro hasta la emisión de tu voto. Esto es importante, más que nunca.

NOTAS

1 • "Texas Media Company Hired By Trump Created Kenyan President's Viral 'Anonymous' Attack Campaign Against Rival, New Investigation Reveals," Privacy International, 15 de diciembre de 2017, visitado el 6 de junio de 2018, https://privacyinternational.org/feature/954/texas-media-company-hired-trump-created-kenyan-presidents-viral-anonymous-attack.

2 • "Biometric Technology, Elections, and Privacy. Investigating Privacy Implications of Biometric Voter Registration in Kenya's 2017 Election Process," CIPIT at Strathmore University, Nairobi, mayo de 2018, visitado el 6 de junio de 2018, https://blog.cipit.org/wp-content/uploads/2018/05/Biometrics-Privacy-Report-by-CIPIT.pdf.

3 • "Report of the Independent Review Commission on the General Elections held in Kenya on 27th December, 2007" (known as the Kriegler Commission), Recommendations Concerning Registration of Voters, p. 157, Kenya Law, 2008, visitado el 6 de junio de 2018, http://kenyalaw.org/kl/fileadmin/CommissionReports/Report-of-the-Independent-Review-Commission-on-the-General-Elections-held-in-Kenya-on-27th-December-2007.pdf.

4 • *Ibid.*, Annex 3.A, pp. 260-295.

5 • *Ibid.*, p. 8.

6 • Agence France-Presse, "Dead Voters and Other Ways to Steal a Kenyan Election." The Daily Nation, 1 de agosto de 2017, visitado el 6 de junio de 2018, https://www.nation.co.ke/news/Kenya-General-Election-2017-and-rigging/1056-4040292-5toedlz/index.html.

7 • Dale T. McKinley and the Right To Know campaign, "New Terrains of Privacy in South Africa." Right2Know, 15 de diciembre de 2016, visitado el 6 de junio de 2018, http://www.r2k.org.za/2016/12/15/research-new-terrains-of-privacy-in-south-africa/.

8 • Dhananjay Mahapatra, "Supreme Court Reserves Verdict on Aadhaar Validity." The Times of India, 11 de mayo de 2018, visitado el 6 de junio de 2018, https://timesofindia.indiatimes.com/india/supreme-court-reserves-verdict-on-aadhaar-validity/articleshow/64116972.cms.

9 • "Biometrics in Kenya's Election," CIPIT blog, 2017, visitado el 27 de marzo de 2018, http://blog.cipit.org/wp-content/uploads/2017/12/Biometrics_history.png.

10 • Dell Cameron, "Private Records of 93.4 Million Mexican Voters Exposed In Data Breach." The Daily Dot, 22 de abril de 2016, visitado el 6 de junio de 2018, http://www.dailydot.com/layer8/amazon-mexican-voting-records/.

11 • Vladimir Hernandez, "Our World: Kidnapped in Mexico." Huffington Post, 15 de marzo de 2017, visitado el 6 de junio de 2018, http://www.huffingtonpost.com/vladimir-hernandez/our-world-kidnapped-in-mexico_b_9462258.html.

12 • "State of Privacy Report for The Philippines," Privacy International, enero de 2018, visitado el 6 de junio de 2018, https://www.privacyinternational.org/state-privacy/1009/state-privacy-philippines.

13 • "Biometric technology, elections, and privacy," CIPIT, mayo de 2018.

14 • Mike Wendling, "The (Almost) Complete History of 'Fake News." BBC, 22 de enero de 2018, visitado el 6 de junio de 2018, http://www.bbc.co.uk/news/blogs-trending-42724320.

15 • Ethan Zuckerman, "The First Twitter Revolution?" Foreign Policy, 24 de marzo de 2011, visitado el 6 de junio de 2018, http://foreignpolicy.com/2011/01/15/the-first-twitter-revolution-2/; Essam Mansour, "The Role of Social Networking Sites (SNSs) in the January 25th Revolution in Egypt," *Library Review* 61, no. 2 (2012): 128-159.

16 • "On the Brink of the Precipice: A Human Rights Account of Kenya's Post-2007 Election Violence," The Kenyan National Commission on Human Rights, 2003, visitado el 6 de junio de 2018, www.knchr.org/Portals/0/Reports/KNCHR_REPORT_ON_

THE_BRINK_OF_THE_PRECIPE.pdf.

17 • "Corporate Responses to Hate Speech in the 2013 Kenya Presidential Elections. Case Study: Safaricom," The Institute for Human Rights and Business, p. 23, noviembre de 2013, visitado el 6 de junio de 2018, https://www.ihrb.org/pdf/DD-Safaricom-Case-Study.pdf.

18 • Por ejemplo, Facebook Business, Homepage, 2018, visitado el 6 de junio de 2018, https://en-gb.facebook.com/business/products/ads/ad-targeting.

19 • La elaboración de perfiles es una expresión descrita en el próximo Reglamento General de Protección de Datos (RGPD) europeo. Es definida como "cualquier forma de procesamiento automatizado de datos personales consistente en utilizar los datos personales para evaluar ciertos aspectos personales relacionados a una persona física, en particular para analizar o predecir aspectos relacionados al rendimiento laboral, situación económica, salud, preferencias personales, intereses, confiabilidad, comportamiento, localidad o movimientos de una persona física". "Article 4 EU GDPR 'Definitions'," Privacy Plan, 2018, visitado el 6 de junio de 2018, http://www.privacy-regulation.eu/en/article-4-definitions-GDPR.htm.

20 • Sean Illing, "Cambridge Analytica, The Shady Data Firm that Might be a Key Trump-Russia Link, Explained." Vox, 17 de marzo de 2018, visitado el 6 de junio de 2018, https://www.vox.com/policy-and-politics/2017/10/16/15657512/cambridge-analytica-christopher-wylie-facebook-trump-russia.

21 • "Letter to Cambridge Analytica on 2017 Kenya Election," Privacy International, 30 de mayo de 2017, visitado el 6 de junio de 2018, https://privacyinternational.org/advocacy-briefing/1683/letter-cambridge-analytica-2017-kenya-election.

22 • "Kenya in 2020 if Raila Odinga is elected President," video de YouTube, 1:28, publicado por The Real Raila, 10 de julio de 2017, visitado el 6 de junio de 2018, https://www.youtube.com/watch?v=o45NlqZXDXw.

23 • "Texas Media Company Hired By Trump...," Privacy International, 2017.

24 • "The Cambridge Analytica Files," The Guardian, marzo de 2018, visitado el 6 de junio de 2018, https://www.theguardian.com/news/series/cambridge-analytica-files.

25 • "Revealed: Trump's Election Consultants Filmed Saying They Use Bribes and Sex Workers to Entrap Politicians," Channel 4 News, at 9", 19 de marzo de 2018, visitado el 6 de junio de 2018, https://www.channel4.com/news/cambridge-analytica-revealed-trumps-election-consultants-filmed-saying-they-use-bribes-and-sex-workers-to-entrap-politicians-investigation.

26 • "Kenyans Bombarded With Fake News in Presidential Election," Channel 4 News, 25 de marzo de 2018, visitado el 6 de junio de 2018, https://www.channel4.com/news/kenyans-bombarded-with-fake-news-in-presidential-election.

27 • "Further Questions on Cambridge Analytica's Involvement in the 2017 Kenyan Elections and Privacy International's Investigations," Privacy International, 27 de marzo de 2018, visitado el 6 de junio de 2018, https://medium.com/@privacyint/further-questions-on-cambridge-analyticas-involvement-in-the-2017-kenyan-elections-and-privacy-15e54d0e4d7b.

28 • Maggie Fick y Alexis Akwagyiram, "In Africa, Scant Data Protection Leaves Internet Users Exposed." Reuters, 4 de abril de 2018, visitado el 6 de junio de 2018, https://www.reuters.com/article/us-facebook-africa/in-africa-scant-data-protection-leaves-internet-users-exposed-idUSKCN1HB1SZ; Nick Miriello, David Gilbert y Julia Steers, "Kenyans Face a Fake News Epidemic." Vice, 22 de marzo de 2018, visitado el 6 de junio de 2018, https://news.vice.com/en_us/article/43bdpm/kenyans-face-a-fake-news-epidemic-they-want-to-know-just-how-much-cambridge-analytica-and-facebook-are-to-blame?utm_campaign=sharebutton; "Kenyans Want to Know What Role Cambridge Analytica Played in their 2017 Presidential Election," Vice News, 22 de marzo de 2018, visitado el 6 de junio de 2018, https://www.youtube.com/watch?v=0xw-DhxNv2Q.

LUCY PURDON – *Reino Unido*
Lucy es oficial de políticas en *Privacy International* y es responsable del desarrollo de políticas. Dirige el trabajo de política mundial sobre seguridad cibernética e identidad. Trabaja en la organización y con colaboradores internacionales para formular recomendaciones y posiciones políticas basadas en las conclusiones de los proyectos de investigación.

contacto: *lucyp@privacyinternational.org*

Recibido en marzo de 2018.
Original en inglés. Traducido por Sebastián Porrua.