APUNTES
3/2018

FRIEDRICH EBERT STIFTUNG BOLIVIA

Datos personales, soluciones colectivas

Sylvain Damien Lesage

Julio, 2018

- Las nociones de privacidad e intimidad están evolucionando en la era de las redes sociales y plataformas digitales. Las huellas digitales que producimos, datos y metadatos, documentan nuestras actividades, sentimientos y relaciones interpersonales. En este sentido, incluyen una dimensión colectiva tradicionalmente ausenta de los mecanismos de protección de los datos "personales".

- Por otra parte, el volumen de datos recolectados por las "plataformas digitales" privadas, nuevos gigantes económicos, proviene de un trabajo humano generalmente invisibilizado, organizado mediante cuatro modos de producción: el micro-trabajo, el trabajo a la demanda, el trabajo "lúdico", y el trabajo "interactivo".

- Frente a las características de la economía digital capitalista, se requieren debates entre trabajadoras y trabajadores, activistas de defensa de los derechos en línea, y representantes de los poderes locales y nacionales, entorno al reconocimiento del valor generado individual y colectivamente, su aprovechamiento, y su redistribución para el desarrollo económico y la justicia social.

Tabla de contenidos

Introducción

No pasa un día sin que se hable de un nuevo escándalo relacionado a los datos personales[1], de la pérdida de privacidad[2], o de la cada vez mayor importancia económica de las empresas tecnológicas[3]. Esto va ligado a la omnipresencia de las tecnologías de la información y comunicación en la vida cotidiana, a la gula de las plataformas tecnológicas por los datos personales, y a la explosión de la cantidad de información colectada, almacenada y explotada.

En Bolivia, dos tercios de la población es internauta. Las telecomunicaciones son un derecho universal, y esas ya no son temáticas de otro mundo. Entran en resonancia con debates políticos recientes sobre la interoperabilidad, el voto electrónico, la regulación de Über o la influencia de las redes sociales en periodos electorales; y al ser partícipes de la producción y entrega masiva de datos a las grandes plataformas globales, crece la concientización y preocupación de las bolivianas y los bolivianos en torno al uso, abuso, pero también valor de los datos personales.

En este artículo, combinamos un análisis de la bibliografía francesa y anglófona con una serie de entrevistas a expertos internacionales y nacionales, para explicitar las problemáticas globales en torno a la privacidad y a la economía de los datos "personales", y así contribuir a nutrir la reflexión sobre la propiedad y el control de estos datos, que tienen la particularidad de ser generados localmente y colectivamente.

Tecnología y procesamiento de los datos

La explosión de los datos a disposición, conocida como *big data*, permite el uso de tecnologías como el aprendizaje automático (*machine learning*), concepto a veces inflado como inteligencia artificial. Abre la vía a aplicaciones de gran impacto, como la medicina predictiva que podría anticipar las epidemias o las enfermedades individuales, o la predicción de crímenes en función a las zonas, los delitos reportados, y otras variables. Pero estas posibles mejoras entran en conflicto evidente con la protección de la privacidad, y también son muy vulnerables a sesgos presentes en los datos utilizados para entrenar a los algoritmos: discriminación a poblaciones particulares, sub-representación de zonas de donde se recaban menos datos (por ejemplo, con una disparidad entre las ciudades y las zonas rurales), hasta sesgo inconsciente de los diseñadores de los algoritmos, o conocimiento insuficiente de la realidad, generando decisiones y clasificaciones imprecisas, binarias o groseras.

La problemática técnica del *big data* amerita otro artículo, pero por lo general, los principales aspectos están listados de manera lúdica con palabras en "v": volumen de los datos a procesar, velocidad del procesamiento contra velocidad del flujo de datos entrantes, variedad de los datos a tratar, veracidad de la información, valor relativo de los datos, vida privada, y otros.

1 Murphy, M. (2018). Twitter caught up in Cambridge Analytica data scandal. The Telegraph, [en línea] 28 de abril. Recuperado de https://www.telegraph.co.uk/technology/2018/04/28/twitter-caught-cambridge-analytica-data-scandal/

2 Véliz, C. (8 de abril de 2018). Tus datos son tóxicos. El País, [en línea] 8 de abril. Recuperado de https://elpais.com/tecnologia/2018/04/06/actualidad/1523030681_007734.html

3 IPO Centre (31 de marzo de 2017). Global Top 100 Companies by market capitalisation. PwC, [en línea] 31 de marzo. Recuperado de https://www.pwc.com/gx/en/audit-services/assets/pdf/global-top-100-companies-2017-final.pdf.

De la misma forma, sin entrar en detalle, el *big data* y los algoritmos han adquirido un rol más importante en las sociedades y, por lo tanto, surgen preocupaciones como la pérdida de control frente a los sistemas automatizados (el ejemplo más impactante son los vehículos autónomos y sus decisiones en caso de accidente[4]); la influencia psicológica de masas (caso Cambridge Analytica, decisiones editoriales de las redes sociales, censura, lucha contra las *fake news*); los sistemas de evaluación de otros humanos (sistema de crédito social del Estado chino, notación de los trabajadores de las plataformas Über o Deliveroo); control y transparencia de los algoritmos, que generalmente se consideran como cajas negras[5](¿será que la única forma de controlar los algoritmos es con otros algoritmos?[6]); o sobre-valuación de los indicadores producidos por los algoritmos en la toma de decisiones políticas[7].

Soluciones técnicas de protección

Frente a los problemas políticos referidos a la defensa de la privacidad, Harry Halpin[8] recomienda soluciones técnicas como la criptografía, las cadenas de bloques y la descentralización, en razón al doble juego de los gobiernos actuales que espían y votan leyes simultáneamente. Halpin sugiere que estas soluciones podrían ser el cimiento de "nuevas formas de vida económica y de gobierno, que tengan que ver a la vez con los mercados libertarianos y con el comunismo consejista, más que con nuestra forma existente de capitalismo". Mallory Knodel [9]destaca también la fuerza de las soluciones tecnológicas a través de los estándares internacionales, generalmente discutidos en asambleas donde reina un consenso en favor de la defensa de los derechos ciudadanos; y cuya aplicación tiene un impacto global, al contrario de las soluciones políticas que ofrecen solamente un impacto local o nacional. Finalmente, Antonio Casilli[10] advierte que si las soluciones tecnológicas son la base, éstas no pueden existir solas, y que su utilización en contextos adversos expone a los ciudadanos a la persecución política, por lo que no entrevé mejoras fuera de un cambio en la educación, una alfabetización informacional y, de manera más amplia, de la formación de seres humanos de calidad, a contrapié de una actual degeneración ideológica.

4 Ver el estudio social en línea de MIT, llamado "Moral Machine", donde los visitantes están invitados a decidir qué personajes de una escena deberían morir en caso de un accidente inevitable. URL: http://moralmachine.mit.edu/

5 Pasquale, F. (2015) The Black Box Society. The Secret Algorithms that Control Money and Information. Cambridge: Harvard University Press.

6 Podemos anticipar una guerra de inteligencia artificial entre plataformas y reguladores, como ya existe en el trading alta frecuencia (HFT) donde los algoritmos luchan entre sí por los tiempos y los precios. Ver http://www.casilli.fr/2012/01/29/antidatamining-or-the-art-of-killing-financial-markets-a-little-every-day/

7 En una entrevista personal el 05/05/2018, Luis Pereira, anterior director del Instituto Nacional de Estadísticas, aclara que Bolivia, al contrario, todavía carece de una cultura de estadísticas, y que los indicadores y mediciones pesan muy poco frente a las intuiciones, percepciones individuales y posiciones ideológicas de los dirigentes.

8 Entrevista personal, 06/05/2018, traducción propia del inglés.

9 Entrevista personal, 05/05/2018, traducción propia del inglés.

10 Entrevista personal, 03/05/2018, traducción propia del francés.

Privacidad y datos personales

Para abordar las problemáticas de los datos personales, importa primero definir el perímetro de la "privacidad" (*o privacy*), la importancia que releva su protección, y los medios que se estén usando para este fin.

Definición de la privacidad

Se requiere discernir el concepto tradicional de la vida privada, de la privacidad "moderna"[11]. La vida privada, o los primeros conceptos de privacidad, se definían en 1890 como "el derecho a que te dejen tranquilo/a"[12] , en referencia a una esfera privada, a la protección frente a las invasiones de otros actores; una entidad íntima que no se tiene que dejar "penetrar" (*privacy as penetration*). En esta visión, la vida privada constituye un núcleo central, y la protección requerida disminuye a medida que se amplía el ambiente, por círculos concéntricos, a las personas cercanas, al grupo social, a la vida profesional y, finalmente, a la vida pública. Sigue el concepto de *privacy as regulation*[13] en el cuál el sujeto establece unas estrategias para defender su derecho a la privacidad, y decide qué parte de su información quiere compartir y con quién. Hasta aquí, las amenazas a la intimidad provienen principalmente de la familia, de la comunidad, o hasta del Estado.

Sin embargo, en la época de las redes sociales y de las plataformas gigantes que lucran con los datos, se vuelve más complicado definir las fronteras de estos círculos concéntricos y de los nuevos espacios que los rodean. La comprensión del entorno y de las consecuencias de los actos en línea se vuelven más difíciles de entender y se procede ahora más por idas y vueltas, prueba y error, con mecanismos de retroalimentación, lo que se conceptualiza como *privacy by negociation*[14], mediante la cual, los individuos trazan las fronteras de su privacidad de manera dinámica y adaptativa.

Características de los datos personales

La parte de la privacidad que nos interesa es la que se relaciona a los datos personales. Definir el concepto de datos personales también es un reto. La ley francesa nº78-17 de enero de 1978, actualizada en 2004, y comúnmente llamada "Ley informática y libertades[15]", no se refiere a datos personales, sino a "datos de carácter personal", que define como "toda información relativa a una persona física identificada o que puede ser identificada, directamente o indirectamente, por referencia a un número de identificación o a uno o varios elementos que le son propios[16]" . En la legislación estadounidense, se hace referencia a la "información personal de identificación"

11 Antonio A. Casilli (2013) Contre l'hypothèse de la « fin de la vie privée. Revue française des sciences de l'information et de la communication, [en línea]. Recuperado de http://journals.openedition.org/rfsic/630; DOI: 10.4000/rfsic.630

12 Warren, S., & Brandeis, L. (1890). The Right to Privacy. Harvard Law Review, 4(5): 193-220.

13 Altman, I. (1977). Privacy regulation: Culturally universal or culturally specific? Journal of Social Issues, 33 (3): 66-84.

14 Donath, J. (2007). Signals in social supernets. Journal of Computer-Mediated Communication, 13(1): 231-251. [En línea]. Recuperado de http://jcmc.indiana.edu/vol13/issue1/donath.html

15 Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. [En línea]. Recuperado de https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=LEGITEXT000006068624

16 Traducción propia del francés.

(*Personally identifiable information – PII*[17]), como "cualquier información sobre un individuo administrada por una agencia, incluyendo (1) cualquier información que pueda ser usada para distinguir o rastrear la identidad de una persona, como su nombre, su número de seguridad social, su lugar y fecha de nacimiento, el apellido materno, o los registros biométricos; y (2) cualquier otra información que está ligada o pueda ser ligada a una persona, como la información médica, educativa, financiera o de empleo" [18]. Finalmente, la Constitución Política del Estado Plurinacional de Bolivia establece la privacidad y la intimidad como derechos civiles, y prevé la Acción de Protección de Privacidad, pero no define conceptos relacionados a los datos personales.

Estas definiciones quedan cortas frente a la realidad de nuestras vidas digitales. Según Mallory Knodel[19], "los datos personales van más allá de la PII. Incluye toda nuestra actividad en línea, prácticamente siempre vinculada con alguna forma de PII, que está registrada, archivada, analizada, compartida, o vendida. Los datos personales se encuentran en nuestras casas, en nuestros propios dispositivos, pero también su naturaleza es de no ser, o de nunca poder ser, en nuestra posesión." Para Antonio Casilli[20], "no hay una gradación entre los datos, en el sentido de abajo y arriba (…), sino que existe una enorme variedad de los datos presentes en la naturaleza, o por lo menos en las plataformas, y además son datos que necesitan, cada uno, (…) y amerita ser tratado de manera diferente". Casilli cita las contraseñas y los códigos PIN como datos secretos no tomados en cuenta por la legislación actual; los datos declarativos como los SMS o los mensajes en Facebook; los datos declarativos "forzados" como el estatus VIH en la aplicación Grindr (esta aplicación compartió la información ultra-sensible con dos compañías, desatando un escándalo mundial[21]); los datos de tipo declarativos, pero pasivos como el rastreo por geolocalización; y los datos calculados por las plataformas. Para Antoinette Rouvroy[22], "la lógica jurídica binaria (según la cual los datos son de carácter personal, o son anónimos) está desfasada de la realidad informática (todo dato clasificado como anónimo siempre presenta un « riesgo » más o menos cuantificable, de « re-identificación »[23]) . Añade que "el problema es la cantidad, y no la calidad de los datos disponibles, por lo que hay que aceptar la cruda realidad: ni el principio del consentimiento individual al tratamiento de los datos personales, ni los sistemas con las mejores intenciones de « privacy by design », son de naturaleza a

17 National Institute of Standards and Technology – NIST (2010) Guide to Protecting the Confidentiality of Personally Identifiable Information (PII). Special Publication 800-122. [En línea]. Recuperado de https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-122.pdf.

18 Traducción propia del inglés.

19 Entrevista personal, 5 de mayo de 2018, traducción propia del inglés.

20 Entrevista personal, 3 de mayo de 2018, traducción propia del francés.

21 El País (2018) Grindr, la 'app' de citas gays, comparte datos de VIH de sus usuarios. El País, [en línea] 3 de abril. Recuperado de https://elpais.com/tecnologia/2018/04/03/actualidad/1522737696_785730.html

22 Rouvroy, A. (2017) Homo juridicus est-il soluble dans les données ? (Preprint). [En línea]. Recuperado de https://www.academia.edu/35166217/Homo_juridicus_est-il_soluble_dans_les_donn%C3%A9es_Is_Homo_juridicus_soluble_in_the_data_

23 A propósito del anonimato de los datos, se recomienda el concepto de k-Anonimity que pretende ofrecer una medición y una garantía del grado de anonimato de un conjunto de datos. Ver Samarati, P.; Sweeney, L. (1998). Protecting privacy when disclosing information: k-anonymity and its enforcement through generalization and suppression. Harvard Data Privacy Lab. [En línea]. Recuperado de https://dataprivacylab.org/dataprivacy/projects/kanonymity/paper3.pdf

frenar el tsunami de los datos".

Aún más interesantes son los datos "sociales", que surgen de una construcción colectiva y representan relaciones entre personas. Pueden ser los datos de un chat, los metadatos[24] de una llamada, o las fotos en la cual aparecen varias personas. En este último caso, las plataformas web que implementan un reconocimiento facial y un cruce de datos, logran generar perfiles "fantasmas" de personas que no son usuarios de la plataforma y que inclusive ignoran que sus datos son recolectados y almacenados. Lo mismo ocurre con las aplicaciones móviles que al instalarse obtienen el acceso al directorio de contactos y al historial de llamadas, develando las relaciones sociales del posesor del dispositivo[25]. Esto implica un cambio en la responsabilidad relacionada a la privacidad, porque una acción individual afecta los datos personales de todas las personas de su entorno digital, sin que éstas sean conscientes, o hayan sido notificadas al respecto. Anshu Sharma[26] denomina esto como transitividad de la privacidad.

Fin legítimo vs oportunismo

Tradicionalmente, los datos recolectados por los Estados y almacenados en los registros administrativos, están regidos por normativas específicas y persiguen un fin legítimo definido antes de realizar la recopilación de la información. En jurisdicciones como Francia, desde 1978, o como Europa, a partir de la entrada en vigencia del Reglamento General de Protección de los Datos – RGPD[27] en mayo de 2018, esta obligación de definir el fin legítimo se aplica también a las empresas que recolectan datos de sus usuarios. El RGPD establece, por ejemplo, que "[l]os datos personales serán (…) recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines". Generalmente, los datos recolectados de esta forma están fuertemente estructurados, con una definición estricta de los campos y de la representación. Ocurre de la misma manera con los datos recolectados en experiencias científicas (saliendo temporalmente del campo de los datos personales), como datos astronómicos, de física de altas potencias, o de cualquier otro proceso experimental con un protocolo muy definido, que producen datos "limpios".

Frente a esta forma tradicional de recolectar y administrar los datos, las plataformas web y los operadores de telecomunicaciones están acumulando cantidades de datos heterogéneos, sin finalidad de recolección previamente definida, de una manera "oportunista" y en formatos desparejos.

24 Los metadatos corresponden a la información que describe los datos, por ejemplo para una llamada telefónica, los números de teléfono, la duración, o la ubicación geográfica de la llamada, por oposición al contenido de la llamada.

25 Aunque usar simplemente un navegador, como Chrome o Firefox, tampoco protege contra la identificación, como lo demuestra el experimento científico AmIUnique (https://amiunique.org/fp) que muestra como el conjunto de metadatos que desvela el navegador crea una huella única para cada usuario.

26 Sharma, A. (2018) Transitive Data Privacy: Behind Golden State Killer DNA and Cambridge Analytica. Medium, [blog en línea] 6 de mayo. Recuperado de https://medium.com/@anshublog/transitive-data-privacy-behind-golden-state-killer-dna-and-cambridge-analytica-a8d6c4ff8452

27 Unión Europea (2016) Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE. [En línea] 27 de abril. Recuperado de https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:32016R0679&from=ES .

Mediante algoritmos de cruce de datos, logran generar indicadores y perfiles a partir de esta masa indeterminada de datos, sin diseño previo. De alguna forma, la misma tendencia aparece con la interoperabilidad entre las entidades públicas. Con el fin de reducir la burocracia percibida por la población, las instituciones intercambian datos de sus diferentes registros administrativos, ahorrándoles a los ciudadanos la necesidad de llevar certificados de un lado a otro. Este esfuerzo coordinado dentro del Estado es una estrategia nueva, no prevista al inicio de las operaciones de los registros administrativos, y con un fin diferente; por lo que viene acompañada de una adaptación del marco normativo de protección de los datos personales.

De la misma forma, según Luis Pereira Stambuk[28], la estadística pública está evolucionando desde las últimas décadas para aprovechar la riqueza de la información provista por los registros administrativos, en un movimiento singular de reflujo. En efecto, hasta el siglo XIX, los registros administrativos, principalmente de población, eran la única fuente para realizar análisis estadísticos, y el siglo XX dio un viraje hacia los censos y las encuestas como los únicos métodos válidos de producción de estadísticas. Finalmente, la profusión de datos proveniente, en particular, del mayor grado de registro de las actividades humanas y económicas por parte de los Estados, motivó un retorno a los registros administrativos como la fuente privilegiada. Cabe notar que aquí también se trata de un aprovechamiento de datos recolectados para otro fin administrativo; no con una finalidad específicamente estadística[29].

28 Entrevista personal, 5 de mayo de 2018.
29 Representa también un ahorro económico sustancial, frente a los censos nacionales.

Recolección de los datos

Un tercer aspecto relacionado a la privacidad de los datos, corresponde al carácter masivo de la recopilación de información. Según Antonio Casilli[30], "el problema de la recolección masiva es un problema frente al cual los estados (…) no han querido posicionarse. (…) Consideraban como (…) una verdad establecida que no se puede interrumpir la recolección, porque es la base del crecimiento económico." Eso genera "un problema de seguridad, con los riesgos de la filtración de datos y de la vigilancia de masa". Para Mallory Knodel[31]:

[L]os gobiernos también se meten en los datos privados, lo que genera un conflicto de interés y puede ser la razón por la cual las leyes, como en Estados Unidos y Canadá, no protegen realmente a la gente. (…) Los gobiernos imponen una vigilancia masiva, aún después de lo que divulgó Snowden. Aplicaron una narrativa de la protección de la población frente a las amenazas en el debate público, y lograron evitar dar respuestas frente a la violación de leyes existentes. (…) Pero lo usaron para recabar información durante campañas electorales y para fines de control de la inmigración, así como para la censura. (…) Las poblaciones vulnerables, los periodistas y los disidentes está afectados de manera desproporcionada por todo eso.

Mientras que surgieron algunos escándalos de vigilancia y persecución política, usando software de empresas como Grey Heron[32],

30 Entrevista personal, 3 de mayo de 2018, traducción propia del francés.
31 Entrevista personal, 5 de mayo de 2018, traducción propia del inglés.
32 Cox, J., Franceschi-Bicchierai L. (2018) New Spyware Company 'Grey Heron' Is Linked to Hacking Team. Motherboard, [en línea] 26 de marzo. Recuperado de https://motherboard.vice.com/en_us/article/bjpnad/grey-heron-hacking-team.

Hacking Team[33] o Amesys[34], diseñados para espiar blancos establecidos[35], el gobierno de Estados Unidos[36] aplica una estrategia holística de vigilancia en todos los estratos de la tecnología, desde la concepción del hardware, pasando por la grabación de las comunicaciones, hasta la obligación por parte de los servicios en línea de entregar la información. Rusia e Irán también realizan una vigilancia masiva de las comunicaciones, a través de aplicaciones nacionales, y censuran torpemente otras aplicaciones que escapan a las escuchas por su carácter cifrado, como Telegram[37]. Francia aprobó medidas de vigilancia masiva en nombre de la lucha contra el terrorismo, en particular con las "cajas negras"[38] que el Estado instala y administra en la infraestructura de los proveedores de acceso a Internet. Finalmente, el gobierno de China, más allá de la censura y de la vigilancia que ejerce sobre la población, llegó a un nivel todavía más alto con el establecimiento de su sistema de crédito social[39] y de tecnologías de vigilancia emocional[40].

La privacidad y la protección de los datos personales ya no pueden ser garantizadas únicamente por el respeto a la intimidad que menciona la Constitución; se requiere considerar la nueva dimensión, fundamental, de los datos como productos sujetos al mercado.

Valor y propiedad de los datos

En 2018, cinco de las diez personas más ricas del mundo obtuvieron su fortuna con las tecnologías de información y comunicación, y dos de ellas a través de servicios cuyo valor deriva directamente de los datos que administran: Facebook mediante la publicidad y Amazon por las recomendaciones de compra[41]. Sin embargo, para Antonio Casilli[42], sería un error considerar que son empresas tradicionales: "no son empresas, son plataformas. (…) La empresa es un fenómeno del siglo XX (…) Las plataformas son en parte una empresa, y en parte un mercado." Casilli explica que

33 Hacking Team (2016) R3D: Red en Defensa de los Derechos Digitales. Red en Defensa de los Derechos Digitales, [en línea] 29 de septiembre. Recuperado de https://r3d.mx/proyecto/hacking-team-en-mexico/.

34 Movimiento Mundial de los Derechos Humanos (2017) Sale of surveillance equipment to Egypt by French company Amesys: impunity must end. MMDH, [en línea] 5 de julio. Recuperado de https://www.fidh.org/en/region/north-africa-middle-east/egypt/sale-of-surveillance-equipment-to-egypt-by-french-company-amesys.

35 Red en Defensa de los Derechos Digitales (2016) El Estado de la Vigilancia – Fuera de Control. [En línea]. Recuperado de https://r3d.mx/wp-content/uploads/R3D-edovigilancia2016-FINAL1.pdf.

36 MacAskill, E., Dance, G. (2013) NSA Files: decoded. The Guardian, [en línea] 1 de noviembre. Recuperado de https://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded.

37 Erdbrink T. (2018) Iran, Like Russia Before It, Tries to Block Telegram App. The New York Times, [en línea] 1 de mayo. Recuperado de https://www.nytimes.com/2018/05/01/world/middleeast/iran-telegram-app-russia.html.

38 Tual, M. (2015) Les députés approuvent le système de surveillance du trafic sur Internet. Le Monde, [en línea] 16 de abril. Recuperado de http://www.lemonde.fr/pixels/article/2015/04/16/les-deputes-approuvent-un-systeme-de-surveillance-du-trafic-sur-internet_4616652_4408996.html.

39 Aldama, Z. (2018) El sistema de crédito social chino salta de la teoría a la práctica. El País, [en línea] 29 de marzo. Recuperado de https://retina.elpais.com/retina/2018/03/27/tendencias/1522145305_569868.html.

40 Chan, T.F. (2018) China is monitoring employees' brain waves and emotions — and the technology boosted one company's profits by $315 million. Business Insider UK, [en línea] 1 de mayo. Recuperado de http://uk.businessinsider.com/china-emotional-surveillance-technology-2018-4.

41 Forbes (2018) The World's Billionaires, 2018 Ranking. Forbes, [en línea]. Recuperado de https://www.forbes.com/billionaires/list/ .

42 Entrevista personal, 3 de mayo de 2018, traducción propia del francés.

las plataformas, en su forma "empresa", permiten la acumulación de riqueza en centros definidos, pero que en su forma "mercado", son el lugar donde la riqueza circula y fluctúa, con precios establecidos automáticamente mediante algoritmos (ver el ejemplo de los precios de taxi de Über[43]).

Producción y generación de valor

Si bien el valor generado por los datos de las plataformas proviene, en parte, de mecanismos de mercado y de comisión sobre las transacciones, también surge del "trabajo digital", o *digital labour*, que se divide en cuatro ecosistemas de producción de los datos[44]. Las plataformas *on-demand* son plazas de mercado de provisión de servicios (Über, Deliveroo. TaskRabbit, Airbnb), con ordenes enviadas en línea y un estatus de independientes para los prestadores de servicios[45]. Las plataformas de microtrabajo hacen realizar tareas muy cortas y específicas a trabajadores para una remuneración mínima (Mechanical Turk), o a usuarios para una remuneración nula (ReCAPTCHA). Las plataformas sociales, como Youtube, Huffington Post o Facebook, recurren al "play bor" (*play y labor*) para hacer generar datos a los usuarios de manera divertida y, generalmente, sin contra-parte económica, a través de los contenidos producidos, de los metadatos de estos usuarios, y del "trabajo del clic" (evaluación de contenidos, reporte de contenidos abusivos). Finalmente, las plataformas *smart* generan masas de datos a partir de dispositivos de tipo Internet de las Cosas, que producen sus datos a partir de las interacciones cotidianas con los usuarios.

Para las plataformas sociales, los usuarios pueden ser considerados como los productos, como lo evoca el famoso lema "[s]i no pagas para ello, no eres un consumidor, eres el producto que se vende"[46], o el dibujo de los "cerditos"[47]: "Cerdos hablando del modelo gratuito. Cerdo 1: ¿No es genial? No tenemos que pagar por el establo. Cerdo 2: ¡Si! Y además la comida es gratuita." La futura adopción del RGPD por la Unión Europea saca esta práctica a la luz, por ejemplo, con el servicio unroll.me, cuyo negocio es la inteligencia de mercado usando las mensajerías de correo electrónico de sus usuarios como materia prima. Este servicio anunció[48] que prefiere borrar las cuentas de sus usuarios europeos antes que cumplir con la reglamentación de protección de datos, demostrando que los usuarios no son sus clientes. Incluso aparecieron servicios dedicados a automatizar el bloqueo de todos los usuarios europeos para las plataformas que no quieren aplicar la reglamentación[49].

43 Fletcher, A. (5 de mayo de 2017) Cómo alcanzar el equilibrio en la uberización económica. Forbes México. [En línea]. Recuperado de https://www.forbes.com.mx/como-alcanzar-el-equilibrio-en-la-uberizacion-economica/.

44 Casilli, A. (2017) Digital Labor Studies Go Global: Toward a Digital Decolonial Turn. International Journal of Communication, 11(2017): 3934–3954.

45 Estatus discutido, con varias decisiones de justicia estableciendo que los "trabajadores independientes" son asalariados de la plataforma, luego de luchas de tipo sindical.

46 Lewis A. (2010) "If you are not paying for it, you're not the customer; you're the product being sold". Twitter, [en línea] 13 de septiembre. Recuperado https://twitter.com/andlewis/status/24380177712.

47 Widder, O. (21 de diciembre de 2010) "The "Free" Model". Geek and Poke. Recuperado de http://geekandpoke.typepad.com/geekandpoke/2010/12/the-free-model.html.

48 Lomas, N. (2018) Unroll.me to close to EU users saying it can't comply with GDPR. TechCrunch, [en línea] 5 de mayo. Recuperado de https://techcrunch.com/2018/05/05/unroll-me-to-close-to-eu-users-saying-it-cant-comply-with-gdpr/.

49 Vincent, V. (2018) Vous pouvez échapper au RGPD en excluant l'Europe de votre site, un service de « gdpr-shield.io ». Developpez.com. [en línea] 4 de mayo. Recuperado de https://www.developpez.com/actu/201597/Vous-pouvez-echapper-au-RGPD-en-excluant-l-Europe-de-votre-site-un-service-de-gdpr-shield-io-propose-de-bloquer-les-utilisateurs-europeens/.

El ingreso que cada usuario de Facebook generó en el primer trimestre de 2018 para la plataforma está evaluado, según cifras de la propia empresa[50], entre 2 y 24 dólares estadounidenses, según su ubicación geográfica. Frente al valor generado, se plantea la cuestión de la redistribución de esta riqueza. Las multinacionales tecnológicas son campeonas en evasión fiscal[51], explotación laboral[52] y puesta en competencia entre ciudades y estados[53].

Venta individual

Una tendencia promovida por pensadores libertarianos[54] o de círculos neoliberales[55] propone que los usuarios de las plataformas reciban un pago por la venta de sus datos personales a las plataformas. Una "falsa buena idea" contra la cual no faltan los argumentos[56]: el monto individual no es muy alto; el poder de negociación de cada individuo contra una plataforma es nulo; al vender los datos, se conceden todos los derechos sobre los datos; un usuario tendrá mucha dificultad para entender las implicaciones presentes y a futuro de la decisión de vender sus datos, hasta la imposibilidad de separar los datos personales en "cajas" independientes, ya que los datos son principalmente relacionales o sociales, y corresponden a varios usuarios. Significa también que yo, individualmente, no puedo hacer mucho para proteger mis datos personales; se requiere necesariamente de una acción colectiva[57], a la manera de las vacunas[58]. Según Irénée Régnauld[59], "aceptar micro-remuneraciones correlacionadas con los datos personales, es grabar en el mármol que las discusiones colectivas se vuelven pequeñas negociaciones individuales". Ella realiza una analogía con el voto: "Pagar para sus datos se parece más a un voto censitario invertido que a un verdadero voto; es una manera de llevar a los analfabetos a la cabina de votación, con el fin de hacerles votar para un proyecto político opaco a cambio de un plato de lentejas."

50 Wagner, K., Molla, R. (2018) Facebook finally has a good day: Business is booming. Recode, [en línea] 25 de abril. Recuperado de https://www.recode.net/2018/4/25/17281500/facebook-fb-mark-zuckerberg-earnings-q1-2018-revenue-stock.

51 Jiménez, M. (2014) Los siete gigantes de Internet pagan en España solo un millón en impuestos. El País, [en línea] 18 de enero. Recuperado de https://elpais.com/economia/2014/01/18/actualidad/1390071860_568641.html.

52 Teknautas (18 de febrero de 2016) Empleados de Amazon denuncian en una web sus pésimas condiciones laborales. El Confidencial, [en línea] 18 de febrero. Recuperado de https://www.elconfidencial.com/tecnologia/2016-02-18/los-empleados-de-amazon-se-desahogan-contra-bezos-en-una-web-anonima_1154360/.

53 El Universal (2017) Apuestan 238 ciudades por sede de Amazon. El Universal, [en línea] 24 de octubre. Recuperado de http://www.eluniversal.com.mx/cartera/economia/apuestan-238-ciudades-por-sede-de-amazon.

54 Simonite, T. (2014) Sell Your Personal Data for $8 a Month. MIT Technology Review, [en línea] 12 de febrero. Recuperado de https://www.technologyreview.com/s/524621/sell-your-personal-data-for-8-a-month/.

55 Schmidtt, F., Madelaine, N. (2018) Gaspard Koenig : « Chaque citoyen doit pouvoir vendre ses données personnelles ». Les Échos, [en línea] 7 de enero. Recuperado de https://www.lesechos.fr/tech-medias/medias/0301069060376-gaspard-koenig-chaque-citoyen-doit-pouvoir-vendre-ses-donnees-personnelles-2142766.php.

56 Monsieur Bidouille (2018). Doit-on etre propriétaire de nos données personnelles ?. Youtube, [video en línea] 30 de abril. Recuperado de https://www.youtube.com/watch?v=D7_MRZwE_PY

57 Idea original. Ver https://twitter.com/mims/status/993478374327758853

58 Idea original. Ver https://twitter.com/slimb0/status/993479846956294144

59 Régnaux, I. (2018) Revendre ses données « personnelles », la fausse bonne idée. Mais où va le web, [en línea] 29 de enero. Recuperado de http://maisouvaleweb.fr/revendre-ses-donnees-personnelles-la-fausse-bonne-idee/.

60 Entrevista personal, 06/05/2018. Traducción propia del inglés.

En el mismo sentido, Harry Halpin[60] rebate la idea de propiedad individual sobre los datos:

Los datos son simplemente las huellas digitales dejadas por tu existencia, y entonces son similares a la extensión digital de tu cuerpo. No *eres dueño* de tu cuerpo, *eres* tu cuerpo. Y entonces, las visiones simplistas sobre la propiedad en relación con los datos no tienen sentido: no se permite a la gente comprar y vender cuerpos, o abandonarlos, es la esclavitud.

Pierre Bellanger[61] sigue la misma analogía interesándose en el "estatus jurídico de la sangre humana, que no puede ser objeto de una comercialización, pero sobre la cual se pueden aplicar derechos de uso consentidos, y que cambian de naturaleza jurídica según qué se encuentra en el interior del cuerpo del individuo, o en el exterior. Este régimen permite entrever un « ser fuera del ser », que podría servir de inspiración para los datos personales".

Negociación colectiva

Para Lionel Maurel y Laura Aufrère[62], es crucial salir del individualismo metodológico, generalmente aplicado a la cuestión de los datos, y elaborar propuestas colectivas, siguiendo la fórmula de Antonio Casilli: "La privacidad dejó de ser un derecho individual para volverse una negociación colectiva"[63]. Estos autores proponen "la construcción de nuevos derechos y un nuevo componente de la protección social, pensado en una solidaridad entre usuarios y trabajadores", imaginando que las Condiciones Generales de Uso (CGU) no se debaten mediante recursos individuales o colectivos en justicia, sino a través de negociaciones colectivas, sobre el modelo de las convenciones colectivas de los sectores laborales entre empresas y trabajadores, utilizando la forma institucional de los sindicatos, que negocian a nombre de quien representan, y cuyos logros en las negociaciones se aplican a todo un sector (en este contexto, una plataforma). Denotan que la escala pertinente para esta organización parece ser la ciudad o la región; niveles territoriales donde la obtención de acceso a los datos amasados por plataformas como Über, Airbnb o Waze, a cambio de la autorización de operar, puede enriquecer la elaboración y el monitoreo de políticas públicas relacionadas a las infraestructuras de transporte, de urbanización o de vivienda.

El mismo Lionel Maurel evoca la idea de Evgeny Morozov[64] de colocar los datos en el "dominio público" para que pertenezcan a la comunidad, haciendo pagar a las plataformas por su uso (de manera práctica, significaría la obligación de las plataformas de abrir una interfaz de programación de

60 Entrevista personal, 06/05/2018. Traducción propia del inglés.

61 Maurel, L. (2014) Comment sortir du paradigme individualiste en matière de données personnelles ? S.I.Lex, [en línea] 19 de julio. Recuperado de https://scinfolex.com/2014/07/19/comment-sortir-du-paradigme-individualiste-en-matiere-de-donnees-personnelles/.

62 Maurel, L., Aufrère, L. (2018) Pour une protection sociale des données personnelles. S.I.Lex, [en línea] 5 de febrero. Recuperado de https://scinfolex.com/2018/02/05/pour-une-protection-sociale-des-donnees-personnelles/.

63 Antonio A. Casilli (2013) « Contre l'hypothèse de la « fin de la vie privée » ». Revue française des sciences de l'information et de la communication, [en línea] 31 de julio. Recuperado de http://journals.openedition.org/rfsic/630

64 Morozov, E. (2016) Data populists must seize our information – for the benefit of us all. The Guardian, [en línea] 4 de diciembre. Recuperado de https://www.theguardian.com/commentisfree/2016/dec/04/data-populists-must-seize-information-for-benefit-of-all-evgeny-morozov. Ver también https://blog.agetic.gob.bo/2017/01/por-un-populismo-digital/.

aplicaciones API de acceso a los datos), y menciona[65] como una pista de aplicación al marco legal de "Bolivia, donde la Constitución permite desde 2009 que los recursos naturales del país se constituyan en una « propiedad social, directa, indivisible e imprescriptible »". En otra publicación[66], Maurel organiza las tesis sobre la relación entre datos personales y comunes, en cuatro categorías[67]: las tesis libristas (software libre, descentralización tecnológica, economía de servicios, para preservar el Internet como un bien común), las tesis colectivistas (instaurar mecanismos colectivos de defensa de los derechos individuales, como acción judicial colectiva de grupo, o sindicatos), las tesis "commonistas" (dar un estatus legal colectivo a los datos, grafos sociales y redes de datos vinculados), y las tesis publicistas (dar un estatus legal de bien público a los datos personales).

Guerra económica

Cabe notar que las plataformas cobraron tal importancia que se volvieron una de las canchas donde se expresa la competencia económica internacional. Según Harry Halpin[68], "el RGPD (…) ha sido adoptado por un deseo de aplicar impuestos a las corporaciones estadounidenses por las invasiones a la privacidad, y para reforzar los competidores europeos, aunque no existen reales competidores europeos." Es "más una barrera comercial a la Silicon Valley en Europa." Otra medida europea parecida fue la multa récord impuesta a Google por "vulnerar la competencia en el mercado de las búsquedas por Internet"[69] . También cabe mencionar el reporte de Collin y Colin[70] que propone "instituir un principio similar al de « *quién contamina paga* (entender impuesto al carbono) » utilizado en fiscalidad medioambiental. Sin exonerar de ninguna manera a las empresas de la obligación de respetar los derechos fundamentales relativos a la protección de los datos personales, este principio « depredador – pagador » conduciría a aplicar impuestos a [las plataformas] que aplican de manera formal al/en el derecho vigente y ejercen en realidad una forma de captación exclusiva de los datos que colectan."

Por su lado, China promueve y favorece a sus propios gigantes de la tecnología, como Alibaba, Baidu, Tencent y Xiaomi[71], en medio de una guerra económica y regulatoria entre

65 Maurel, L. (2017) Evgeny Morozov et le « domaine public » des données personnelles. S.I.Lex, [en línea] 29 de octubre. Recuperado de https://scinfolex.com/2017/10/29/evgeny-morozov-et-le-domaine-public-des-donnees-personnelles/

66 Maurel, L. (2017) Données personnelles et Communs: une cartographie des thèses en présence. S.I.Lex, [en línea] 15 de noviembre. Recuperado de https://scinfolex.com/2017/11/15/donnees-personnelles-et-communs-une-cartographie-des-theses-en-presence/

67 Ver el mapa mental "Données personnelles et Communs: une cartographie des thèses en présence", con una exhaustiva lista de referencias hacia las posiciones y propuestas expresadas en relación al estatus jurídico de los datos personales. [En línea]. Recuperado de https://www.mindmeister.com/es/981161846?t=ONagi5GY5H.

68 Entrevista personal, 06/05/2018, traducción propia del inglés.

69Abellán, L. (2017) Bruselas sanciona a Google con una multa récord de 2.424 millones de euros. El País, [en línea] 27 de junio. Recuperado de https://elpais.com/economia/2017/06/27/actualidad/1498554639_549183.html

70 Collin, P., Colin, N. (2013) Mission d'expertise sur la fiscalité de l'économie numérique. Ministère de l'Économie et des Finances/Ministère du redressement productif. [En línea]. Recuperado de http://6ix-it.com/wp-content/uploads/2013/01/rapport-COLLIN-COLLIN.Donnees.Personnelles.pdf

71 Greeven, M., Wei, W. (2017) Meet China's new tech giants: Alibaba, Baidu, Tencent and Xiaomi. The Telegraph, [en línea] 17 de octubre. Recuperado de https://www.telegraph.co.uk/news/world/china-watch/technology/new-technology-giants/.

China y Estados Unidos[72] [73] [74]. Rusia también impulsa sus redes sociales como VKontakte[75], y ha definido su propia doctrina relativa a la información[76], la cual engloba seguridad de la información, estrategia mediática, y hasta aspectos culturales y psicológicos.

Datos abiertos

Salgamos un momento del tema de los datos estrictamente personales para abordar los datos abiertos, u open data, y su impacto económico. Para Pierre Gautreau[77], los Estados invierten en la producción, armonización y publicación de sus datos con varios objetivos, según los países: legitimidad y prestigio; efecto simbólico; transparencia y rendición de cuentas; fomento a la creación de aplicaciones y servicios en el sector privado; o participación democrática y empoderamiento de los pueblos. Pero para él y para Antonio Casilli[78], raras son las evaluaciones del impacto económico de los datos abiertos [79] [80] [81], y el esfuerzo de los Estados parece estar motivado por otros criterios, como la apuesta, el efecto de moda, y tal vez ante todo por el "efecto vergüenza", tanto a nivel de los funcionarios, como de los mismos Estados, de no ser el último en liberar los datos.

Conclusión

El presente artículo fue concebido como un panorama introductorio sobre las características y los retos de la privacidad y de la economía de los datos personales. Las nuevas dimensiones consideradas, más allá del tradicional derecho a la intimidad, podrían alimentar reflexiones e investigaciones en Bolivia.

En el contexto de la modernización del Estado boliviano, a través de mecanismos de interoperabilidad, de digitalización y de administración de datos personales, se instaló un debate político en torno a las condiciones de intercambio de la información, a la seguridad de la información, a la protección de la privacidad, y al consentimiento de los ciudadanos para el uso de sus datos. Algunos conceptos como la minimización de los datos recolectados, la justificación de la recopilación de datos por un fin legítimo, y el derecho de acceso y corrección de los datos personales, podrán ser estudiados para una adecuación normativa, tanto para reglamentar la administración de datos

72 El Mañana (2018) Estados Unidos prohíbe a empresas vender componentes a ZTE. El Mañana, [en línea] 16 de abril. Recuperado de https://www.elmanana.com/estados-unidos-prohibe-empresas-vender-componentes-zte-zte-estados-unidos-washington/4377394

73 Shaban, H. (2018) Pentagon tells U.S. military bases to stop selling ZTE, Huawei phones. The Washington Post, [en línea] 2 de mayo. Recuperado de https://www.washingtonpost.com/news/the-switch/wp/2018/05/02/pentagon-tells-u-s-military-bases-to-stop-selling-zte-huawei-phones/

74 A matizar, con el hecho de que la mayoría de los dispositivos de marcas estadounidenses siguen siendo fabricados en suelo chino.

75 Yegórov, O. (2016) VKontakte, la red social rusa que planta cara a Facebook. Russia Beyond, [en línea] 20 de octubre. Recuperado de https://es.rbth.com/technologias/informatica/2016/10/20/vkontakte-la-red-social-rusa-que-planta-cara-a-facebook_640523

76 Lawson, S. (2016) Russia Gets A New Information Security Doctrine. Forbes, [en línea] 9 de diciembre. Recuperado de https://www.forbes.com/sites/seanlawson/2016/12/09/russia-gets-a-new-information-security-doctrine/

77 Entrevista personal, 05/05/2018.

78Entrevista personal, 03/05/2018, traducción propia del francés.

79 World Wide Web Foundation (2016) Open Data Barometer Global Report (Fourth Edition). [En línea]. Recuperado de http://www.opendatabarometer.org.

80 Young, A. y Verhulst, S. (2016) The Global Impact of Open Data: Key Findings from Detailed Case Studies Around the World. [e-book] O'Reilly. Recuperado de https://www.safaribooksonline.com/library/view/the-global-impact/9781492042785/.

81 GOVLAB. Open Data's Impact. [En línea] Recuperado de http://odimpact.org/.

personales por parte del Estado, como para ampliar el marco existente a los servicios privados.

El caso de las plataformas globales con usuarios -y eventualmente operaciones comerciales- en Bolivia como Facebook/ Whatsapp/Instagram, Google/Youtube, Über, Airbnb, o Amazon, en una cierta medida, amerita reflexiones más estratégicas por la dificultad de poder influir sobre estos gigantes. En primer lugar, se podrá trabajar en mecanismos de retroalimentación a la sociedad boliviana por el valor que se genera desde el país, como impuestos y apertura de datos o servicios, eventualmente en coordinación con otros países de la región, de manera que el mercado en juego sea suficientemente grande para que las plataformas se sometan a las regulaciones. Otro tipo de estudio se orientaría a entender si el modelo de empresa o de plataforma fuertemente basado en datos podría aplicarse a empresas nacionales, o si se requiere una dimensión global para cobrar eficiencia.

En el contexto de las tecnologías diseñadas con la vigilancia y el espionaje como modelo de negocio desde las grandes potencias (EEUU, China), se podrían imaginar alianzas y colaboraciones entre los Estados que deseen proteger su soberanía, y comunidades de la sociedad civil, en torno a conceptos tecnológicos como la descentralización, el software libre, el hardware libre, la criptografía, o las cadenas de bloques.

Por último, los contornos mismos de la noción de privacidad quedan por definir, cuestionando las diferencias entre privado y privatizado (la propiedad sobre los datos no implica necesariamente su mercantilización), o entre público y publicado (la administración de datos personales por parte del Estado no implica un uso irrestricto). Se podrá considerar también el consentimiento individual y el carácter íntimo de los datos personales, frente a la presión social que orienta los usos en línea, y la necesidad de actuar colectivamente para entender los riesgos (mediante educación y alfabetización digital, para que la privacidad no sólo sea para privilegiados) y negociar la protección de los datos.

Autor:

Sylvain Damien Lesage desarrollador especialista en análisis y visualización de datos geográficos. Fue director ejecutivo de la Agencia para el Desarrollo de la Sociedad de la Información en Bolivia - ADSIB.

Pie de imprenta

Friedrich-Ebert-Stiftung Bolivia

Av. Hernando Siles C/14 Obrajes N° 5998

La Paz - Bolivia

ISBN: 978-99974-0-246-2
DL: 4-4-2122-18

Contacto

Tel: +591 2-2750005
Fax: +591-2-2750090
www.fes-bolivia.org
info@fes-bolivia.org
Facebook: Fundación Friedrich Ebert Bolivia
Twitter: @BoliviaFes