RASTREADORES EN APLICACIONES DE ALIMENTACIÓN Y DIETA

Una comparación entre Chile y Uruguay

DERECHOS DIGITALES
América Latina

RASTREADORES EN APLICACIONES DE ALIMENTACIÓN Y DIETA:
Una comparación entre Chile y Uruguay

Esta publicación fue realizada por Derechos Digitales, con el apoyo de Privacy International.

Derechos Digitales es una organización independiente y sin fines de lucro, fundada en el año 2005, cuya misión es la defensa, promoción y desarrollo de los derechos fundamentales en los entornos digitales en América Latina.

Investigación por María Encalada y Miguel Flores.
Texto por María Encalada, Miguel Flores, Ileana Silva y Vladimir Garay.

Septiembre 2023

Esta obra está disponible bajo licencia Creative Commons Attribution 4.0 Internacional
https://creativecommons.org/licenses/by/4.0/deed.es

ÍNDICE

DESCRIPCIÓN DE LA INVESTIGACIÓN

Como una organización trabajando en la intersección entre las nuevas tecnologías digitales y los derechos humanos, durante los últimos años Derechos Digitales ha realizado distintos esfuerzos de investigación e incidencia en favor del derecho a la privacidad y la protección de los datos personales.

En ese marco, fuimos invitados por Privacy International a participar de una investigación respecto de servicios y aplicaciones web, los datos que recaban y la participación de rastreadores o *data brokers* en ese proceso.

Los rastreadores, también conocidos como "corredores de datos" e "intermediarios de datos", son piezas de software cuya tarea es reunir información sobre la persona que utiliza una aplicación, el modo en que la usan y el dispositivo en el que la aplicación se está ejecutando. Por este motivo, hay consideraciones relativas al ejercicio del derecho a la privacidad y a la protección de datos personales que entran en juego.

Nuestro interés particular para esta investigación era realizar una comparación, con la finalidad de observar diferencias sustantivas en la manera en que las aplicaciones recolectan información en países con distintos estándares de protección en materia de datos personales. Así, decidimos trabajar sobre cinco aplicaciones en dos países: Chile y Uruguay.

En acuerdo con Privacy International, decidimos analizar aplicaciones para teléfonos móviles con foco en alimentación y pérdida de peso.

Las aplicaciones seleccionadas fueron Habits , Lifesum, Fitia, Fasting Tracker y Simple: Ayuno intermitente.

Para llevar a cabo la revisión utilizamos un entorno propuesto por Privacy International para la interceptación de datos (Data Interception Environment),[1] el que nos permitió interceptar la comunicación entre aplicaciones y servidores, las peticiones HTTP enviadas. Además, hicimos uso de Exodus,[2] plataforma de revisión estática de código de aplicaciones para Android, que nos permitió contrastar nuestros resultados. Trabajamos en teléfonos virtuales, desde donde establecimos las ubicaciones e instalamos las aplicaciones.

PREGUNTA DE INVESTIGACIÓN

La pregunta que guía esta investigación es: ¿existen diferencias relevantes en el funcionamiento de rastreadores en aplicaciones web que tengan relación con los diferentes estándares normativos vigentes en Uruguay y Chile en materia de protección de datos personales?

---

1. https://privacyinternational.org/learn/data-interception-environment

2. https://exodus-privacy.eu.org

NORMATIVAS VIGENTES: URUGUAY Y CHILE

Uruguay

En Uruguay, el derecho a la protección de datos personales está amparado en la Ley Nº 18.331 de 2008.[3] En su artículo 1, la ley declara que la protección de los datos personales constituye un derecho es inherente a la persona humana, por lo que está comprendido en el artículo 72 de la Constitución de la República.[4] La Ley reconoce el derecho a controlar el uso que se hace de los datos personales. Se aplica a los datos personales registrados en cualquier soporte que permita tratarlos y usarlos posteriormente de diversos modos, tanto en el ámbito privado como público.

El énfasis está en el rol de la protección de datos como derecho facilitador de otros derechos y libertades. Dentro de los principios que orientan el uso de datos personales en Uruguay,[5] se encuentra la garantía de protección de los datos de las personas, sin importar nacionalidad o residencia. La ley identifica además datos que por sus características deben ser especialmente protegidos, como bases de datos con fines publicitarios o los datos relativos a la actividad comercial o crediticia. Se extiende el catálogo de datos sensibles para incluir los genéticos y biométricos, entre otros. Se incluye la referencia al tratamiento no automatizados de datos, y se excluye del ámbito del Convenio el tratamiento doméstico de datos personales. Se regulan aspectos relacionados a la seguridad de los datos y la transparencia en su tratamiento.

Desde su promulgación, la ley ha sido objeto de continuas actualizaciones y mejoras. En 2013, por medio de la ley 19.030,[6] Uruguay aprueba el Convenio N° 108 del Consejo de Europa para la protección de las Personas con Respecto al Tratamiento Automatizado de Datos de Carácter Personal de 28 de enero de 1981, adoptado en Estrasburgo, y el Protocolo Adicional al Convenio para la Protección de las Personas con Respecto al Tratamiento Automatizado de Datos de Carácter Personal, a las Autoridades de Control y a los Flujos Transfronterizos de Datos, adoptado en Estrasburgo el 8 de noviembre de 2001. De esta manera, se convirtió en uno de los países latinoamericanos en obtener el máximo nivel de protección de los datos personales acorde con la legislación más avanzada en la Comunidad Europea.[7]

---

3. https://www.impo.com.uy/bases/leyes/18331-2008

4. https://www.impo.com.uy/bases/constitucion/1967-1967/72

5. https://www.gub.uy/unidad-reguladora-control-datos-personales/sites/unidad-reguladora-control-datos-personales/files/documentos/publicaciones/guia-1-web.pdf

6. https://www.impo.com.uy/bases/leyes-originales/19030-2012

7. https://galantemartins.com/uruguay-avanza-en-la-proteccion-de-datos-personales-con-estandar-europeo/

Chile

En Chile, la protección de los datos personales se rige actualmente por la Ley Nº 19.628. Sobre protección de la vida privada[8] de 1999, que regula el trato de los datos de carácter personal, en registros o bancos de datos, tanto por organismos públicos como privados. Además, en el año 2018, mediante la ley 21.096, se agrega al numeral 4 del artículo 19[9] de la Constitución Política de la República una mención explícita sobre la protección de los datos personales, adquiriendo carácter de derecho fundamental.

La ley Nº 19.628 de 1999 fue la primera legislación en materia de datos personales en América Latina. Sin embargo, existe consenso en la doctrina de que la legislación chilena otorga un esquema débil para la protección de los datos personales y sus titulares.[10] En ese sentido, la ley se entiende mejor como un marco regulatorio para el mercado de las bases de datos que como un instrumento efectivo para la protección de los derechos de las personas en relación a su información personal.

A pesar de la convicción generalizada que parece haber en el país respecto de la necesidad de reemplazar la normativa por una regulación que considere tanto los desafíos que impone la masificación de las tecnologías digitales desarrolladas durante las dos últimas décadas, como el carácter de derecho fundamental conferido a la protección de los datos personales mediante la reforma constitucional, a la fecha ha sido imposible promulgar una nueva ley.

Si bien la tramitación de la normativa ha sido postergada en distintas ocasiones, durante 2023 se han logrado avances relevantes, que apuntan a una resolución en el corto plazo.[11] A principios de mayo, la Cámara de Diputados aprobó el proyecto que garantiza a todas las personas el acceso, rectificación, supresión, oposición, portabilidad y bloqueo de sus datos personales, en tanto derechos de carácter personal, irrenunciable, que no puede limitarse por ningún acto o convención. Además, el proyecto crea una Agencia de Protección de Datos Personales, junto a una serie de otras mejoras relevantes, que deberán ser aprobadas por el Senado.

En el intertanto, la marcada diferencia entre el estándar de protección actual entre Chile y Uruguay ofrece una oportunidad interesante para realizar una comparación respecto de su capacidad para introducir (o no) cambios relevantes respecto a las prácticas de los distintos actores, en favor de una mejor protección de las personas.

---

8. https://www.bcn.cl/leychile/navegar?idNorma=141599

9. https://www.bcn.cl/leychile/navegar?idNorma=242302

10. Para un análisis más completo sobre la ley Nº 19.628, sugerimos revisar el documento "El estado de la protección de los datos personales en Chile" en https://www.derechosdigitales.org/wp-content/uploads/PVB-datos-int.pdf

11. https://www.camara.cl/cms/noticias/2023/05/08/tratamiento-de-datos-personales-tendra-nuevo-marco-legal/

Específicamente, buscamos observar si la recolección de datos funciona de manera diferente en las mismas aplicaciones en uno u otro país. Entendemos que el mérito de una legislación no puede ser medido simplemente en un ejercicio de este tipo y que cualquier conclusión a la que podamos llegar no será más que el punto de partida para futuros esfuerzos de investigación. Sin embargo, por acotados que sean los resultados, nos parece una perspectiva interesante de abordar.

EXPLICACIÓN DE LA METODOLOGÍA

Para realizar el análisis de las aplicaciones, se utilizaron las herramientas[12] y la metodología propuesta por Privacy International:[13]

- Todas las aplicaciones se instalaron en teléfonos móviles Android, emulados con Genymotion.[14]
- Se utilizó el GPS de Genymotion para configurar las ubicaciones donde se probarían las aplicaciones (Uruguay y Chile).
- Se configuraron las aplicaciones, creando cuentas de usuarios en cada una.
- Se restringió el acceso a internet a las aplicaciones durante los análisis mediante una aplicación móvil (netguard) para separar el tráfico entre una y otra.
- Para realizar el análisis del tráfico de cada una de las aplicaciones se usó el Entorno de Interceptación de Datos de Privacy Intenational, realizando una inspección manual con mitmproxy[15] mediante la implantación de un certificado de raíz con el fin de poder descifrar las comunicaciones.
- Se realizó un análisis del tráfico de red, con el objetivo de determinar con qué instancias se compartían datos. No se inspeccionó el código de las aplicaciones ni se modificaron las peticiones.
- Durante el proceso de análisis no fue posible aislar por completo el tráfico de cada aplicación sin descartar tráfico del core de Android, por lo que hubo que revisar manualmente los registros de tráfico para descartar solicitudes a servidores no provenientes de la app estudiada.

12. https://github.com/privacyint/appdata-environment-desktop/tree/update-3

13. https://privacyinternational.org/video/4719/video-how-use-data-interception-environment

14. https://www.genymotion.com/

15. https://mitmproxy.org/

- Una vez realizado el análisis de tráfico de cada aplicación, se procedió a la comparación con los informes generados por Exodus (uno para cada aplicación), que arrojaron los principales datos vinculados al uso de la información personal ingresada por los usuarios.

DESCRIPCIÓN DE LA MUESTRA

La muestra fue seleccionada de entre las aplicaciones disponibles en la categoría "Planificación de comidas", disponibles en la Play Store de Chile y Uruguay, que tuvieran más de 1 millón de descargas y que solicitaran datos personales de las y los usuarios.

Las aplicaciones escogidas fueron Fasting Tracker, Fitia, Habits/Loop - Analizador de Hábitos,[16] Lifesum y Simple: Ayuno intermitente.

Descripción de las aplicaciones

FASTING TRACKER (VERSIÓN 1.6.2)[17]

Es una aplicación de seguimiento de ayuno. En sus propias palabras "te guía en un nuevo estilo de vida con hábitos saludables". Cuentan con más de 10 millones de descargas.

En su página de Google Play, se indica que los datos que esta aplicación puede recoger son nombre y correo electrónico, actividad en la aplicación, interacciones de la aplicación, información y rendimiento de aplicaciones, registros de fallos y diagnósticos, y IDs de dispositivo o de otro tipo.

En cuanto a la seguridad de los datos, indica que "las prácticas relacionadas con datos pueden variar en función de la versión de la aplicación, el modo en que la utilices, la región donde vayas a usarla y tu edad".

Además, el equipo desarrollador indica que esta aplicación no comparte datos de usuario con otras empresas u organizaciones. Indica que también que los datos se cifran en tránsito y que se transfieren a través de una conexión segura. Los usuarios pueden solicitar que se eliminen los datos.

FITIA (VERSIÓN 14.2.3)[18]

Fita es una aplicación que "crea planes nutricionales para bajar de peso, ganar músculo o simplemente para que comas mejor. Potenciado con un contador de calorías con más de 400,000 productos verificados y más de 6,000 recetas saludables".

Cuenta con más de 5 millones de descargas.

---

16. La misma aplicación tiene diferente nombre en Chile (Habits) y en Uruguay (Loop - Analizador de Hábitos)

17. https://play.google.com/store/apps/details?id=bodyfast.zero.fastingtracker.weightloss

18. https://play.google.com/store/apps/details?id=com.nutrition.technologies.Fitia

Según indican en su perfil de GooglePlay, los datos que recoge la aplicación son correo electrónico, funcionalidad de la aplicación y gestión de cuentas, IDs de usuario, funcionalidad de la aplicación, análisis, Comunicaciones del desarrollador y Gestión de cuentas, información de actividad física, interacciones de la aplicación, análisis y publicidad o marketing, historial de búsquedas en la aplicación, funcionalidad de la aplicación y personalización

En el mismo perfil, indican que el desarrollador de esta aplicación no comparte datos de usuario con otras empresas u organizaciones. Los datos se cifran en tránsito y se transfieren a través de una conexión segura. Los usuarios pueden solicitar que se eliminen los datos.

HABITS/LOOP ANALIZADOR DE HÁBITOS (VERSIÓN 2.0.3)[19]
Se promociona como una aplicación que: "ayuda a crear y mantener buenos hábitos, permitiéndote alcanzar tus metas a largo plazo". Detallados gráficos y estadísticas muestran como los hábitos mejoran con el tiempo. No tiene anuncios publicitarios y es de código abierto.

Tiene actualmente más de 5 millones de descargas.

En su perfil de Google Play, indican que esta aplicación no recoge ni comparte datos de usuarios con otras empresas u organizaciones.

LIFESUM (VERSIÓN 12.2.0)[20]
Es una aplicación que funciona como contador de calorías. Según su propia definición "te ayuda a adoptar dietas nutritivas que se adaptan a tus gustos y a tu estilo de vida. Consigue tus objetivos de pérdida de peso al mismo tiempo que creas unos hábitos de comida saludables para toda la vida".

Cuentan con más de 10 millones de descargas.

En esta aplicación, los desarrolladores declaran recoger los siguientes datos personales: nombre, correo electrónico, IDs de usuario; análisis, publicidad o marketing y personalización, historial de compras, información de actividad física, fotos y videos, interacciones de la aplicación, historial de búsquedas en la aplicación y IDs de dispositivo. En su perfil, aseguran que los datos se cifran en tránsito y que se puede solicitar el borrado de los datos personales.

SIMPLE: AYUNO INTERMITENTE (VERSIÓN 6.4.64)[21]
Se trata de una aplicación "para controlar el ayuno intermitente, adelgazar, beber agua y buscar comidas".

Actualmente cuentan con más de 1 millón de descargas.

---

19. https://play.google.com/store/apps/details?id=org.isoron.uhabits&pli=1

20. https://play.google.com/store/apps/details?id=com.sillens.shapeupclub

21. https://play.google.com/store/apps/details?id=life.simple

Según indican los desarrolladores, la información personal de los usuarios recogida por esta aplicación, es: nombre, correo electrónico, IDs de usuario, información de salud, información de actividad física, funcionalidad de la aplicación, fotos, interacciones de la aplicación, aplicaciones instaladas y IDs de dispositivo.

Además, se señala que los datos se cifran en tránsito y se transfieren a través de una conexión segura. Los usuarios pueden solicitar a los desarrolladores que se eliminen sus datos personales.

RESULTADOS

El análisis de tráfico en cada una de las aplicaciones se realizó usando el Entorno de Interceptación de Datos de Privacy International aplicando mitmproxy.[22]

Se obtuvieron capturas de cada prueba ejecutada, se filtró el tráfico y se comparó el resultado con el análisis de Exodus Privacy,[23] un sitio que permite identificar, a través de un análisis estático de código, rastreadores y permisos de aplicaciones Android.

FASTING TRACKER

En el análisis de esta aplicación, no se identifican llamadas a servidores de Facebook. Sin embargo, se encuentran llamadas a Google, de la misma forma en ambos países, tal como se describe en el reporte de la plataforma Exodus.[24]

Los rastreadores identificados en el análisis de esta aplicación son: Facebook Ads, Google AdMob, Google CrashLytics, Google Firebase Analytics

FITIA

En esta aplicación, se comparten datos con los mismos rastreadores en ambas instancias (Chile y Uruguay). Los rastreadores que se identificaron esta aplicación son: Facebook Ads, Facebook Analytics, Facebook Login, Facebook Share, Google AdMob, Google Analytics, Google CrashLytics, Google Firebase Analytics, Google Tag Manager, Singular.

De los rastreadores declarados en Exodus[25] no se identificaron llamadas a MixPanel[26] o a OpenTelemetry.[27] Sin embargo, pudimos ver en ambos casos llamados a

---

22. https://mitmproxy.org/

23. https://exodus-privacy.eu.org/

24. https://reports.exodus-privacy.eu.org/es/reports/315422/

25. https://reports.exodus-privacy.eu.org/es/reports/347986/

26. https://mixpanel.com/

27. https://opentelemetry.io/

https://api.qonversion.io/, una plataforma de almacenamiento de datos para aplicaciones móbiles, Qonversion.[28]

HABITS/LOOP - ANALIZADOR DE HÁBITOS

El análisis de esta aplicación refleja que la misma no genera ningún tipo de notificación a servidores externos. Es decir, que almacena todo de manera local, en ambas instalaciones (Chile y Uruguay). Esto se condice con el informe de Exodus[29] sobre la app.

LIFESUM

Los rastreadores que pudimos identificar que utiliza esta aplicación son: Adjust, Branch, Braze (formerly Appboy), Facebook Analytics, Facebook Login, Facebook Share, Google CrashLytics, Google Firebase Analytics, HelpShift.

Según nuestro análisis, y en contraste con el reporte de Exodus,[30] ni en Chile ni en Uruguay, esta aplicación genera el llamado a *branch.io* detectable por regla de red.

El resto de las llamadas suceden de igual forma en ambas instalaciones hacia las mismas instancias de rastreadores, a excepción del antes mencionado.

SIMPLE: AYUNO INTERMITENTE

Los rastreadores que se identificaron en esta aplicación son: Amplitude, AppsFlyer, Braze (formerly Appboy), Facebook Analytics, Facebook Login, Facebook Share, Google CrashLytics,Google Firebase Analytics.

En esta aplicación se corroboran los datos de rastreadores reportados por Exodus[31] en ambos casos. Además, en ambos casos se envían datos personales seteados en la app al servidor *rest.fstr.app*, que corresponde a una API. No fue posible corroborar si se trata de servidores exclusivos de la app o una instancia de arriendo (compartida o tercerizada).

Esta es la única app analizada en la que encontramos diferencias entre el comportamiento de la instalación en Chile y la instalación en Uruguay. En el caso de Chile aparecen datos compartidos con el servidor https://m.stripe.com/,una infraestructura financiera para internet - (https://stripe.com/es-us). En el caso de la aplicación ejecutada georeferenciada en Uruguay esa comunicación no se generó.

Además de lo anterior, se comparten datos con el servidor https://api.revenuecat.com, correspondiente a (In-App Subscriptions Made Easy - https://www.revenuecat.com/).

---

28. https://qonversion.io/

29. https://reports.exodus-privacy.eu.org/es/reports/213447/

30. https://reports.exodus-privacy.eu.org/es/reports/312609/

31. https://reports.exodus-privacy.eu.org/es/reports/336843/

Comparativo de rastreadores por aplicación

Aplicación / Rastreador	Fasting Tracker	Fitia	Habits	Lifesum	Simple: Ayuno intermitente
Adjust				X	
Amplitude					X
AppsFlyer					X
Branch				X	
Braze (formerly Appboy)				X	X
Facebook Ads	X	X			
Facebook Analytics		X		X	X
Facebook Login		X		X	X
Facebook Places					
Facebook Share		X		X	X
Google AdMob	X	X			
Google Analytics		X			
Google CrashLytics	X	X		X	X
Google Firebase Analytics	X	X		X	X
Google Tag Manager		X			
HelpShift				X	
MixPanel					
Singular		X			

Listado de peticiones por aplicación, rastreador y país:

A continuación, se resumen las peticiones hechas desde las aplicaciones analizadas por rastreadores. El número de peticiones varía entre Chile y Uruguay, algunas de las peticiones son repetidas pero incrementales, es decir, en la primera petición envía las llaves sin valor y en las peticiones posteriores agrega valores, incluso se observó que estos cambiaban entre una y otra.

Además, en Datos compartidos, no se detallan todos los parámetros del cuerpo de las peticiones, solo se mencionan los más representativos a criterios del equipo.

CHILE		URUGUAY	
Fitia			
api.qonversion.io 4 peticiones	access_token	api.qonversion.io 3 peticiones	access_token
	advertiser-id		advertiser-id
	purchases		purchases
	receipt		receipt
	history		history
	products_local_data		products_local_data
www.facebook.com 1 petición	prefetch_urls	www.facebook.com 1 petición	prefetch_urls
	app_started_reason		app_started_reason
	SDK_CAPABILITY		SDK_CAPABILITY
	CLIENT_REQUEST_ID		CLIENT_REQUEST_ID
	DATA_PROCESSING_ OPTIONS_COUNTRY		DATA_PROCESSING_ OPTIONS_COUNTRY
	DATA_PROCESSING_ OPTIONS_STATE		DATA_PROCESSING_ OPTIONS_STATE
graph.facebook.com 4 peticiones incremental	anon_id	graph.facebook.com 1 petición	anon_id
	advertiser_id		advertiser_id
	access_token		access_token
	billing_client_lib_included		billing_client_lib_included
	implicitlyLogged		implicitlyLogged
	_session_id		_session_id
app-measurement.com	no legible		no aplica
Fasting			
app-measurement.com 1 petición	no legible	app-measurement.com 1 petición	no legible
Lifesum			
graph.facebook.com 3 peticiones	anon_id	graph.facebook.com 3 peticiones	anon_id
	application_tracking_enabled		application_tracking_enabled
	advertiser_id_collection_ enabled		advertiser_id_collection_ enabled
	advertiser_id		advertiser_id
	advertiser_tracking_enabled		advertiser_tracking_enabled
	access_token		access_token
	fb_mobile_launch_source		fb_mobile_launch_source
	fb_mobile_pckg_fp		fb_mobile_pckg_fp
	fb_mobile_app_cert_hash		fb_mobile_app_cert_hash
sdk.fra-01.braze.eu 11 peticiones incremental	api_key	sdk.fra-01.braze.eu 6 peticiones	api_key
	device_id		device_id
	session_id		session_id
	device		device
	push_token		push_token
	user_id		user_id
app-measurement.com 3 peticiones	no legible	app-measurement.com 2 peticiones	no legible

CHILE		URUGUAY	
Simple: Ayuno intermitente			
sdk.iad-05.braze.com 9 peticiones	api_key	sdk.iad-05.braze.com 9 peticiones	api_key
	device		device
	device_id		device_id
	session_id		session_id
	user_id		user_id
	push_token		push_token
	Información general del perfil (nombre, género, foto, email)		Información general del perfil (nombre, género, foto, email)
	product_android_price		product_android_price
	product_android_weekly_ price		product_android_weekly_ price
	product_android_id		product_android_id
	product_android_ introductory_price		product_android_ introductory_price
graph.facebook.com 1 petición	no legible	graph.facebook.com 1 petición	no legible
app-measurement.com 2 peticiones	no legible	app-measurement.com 2 peticiones	no legible
api.revenuecat.com 1 petición	$appsflyerId	api.revenuecat.com 1 petición	$appsflyerId
	$gpsAdId		$gpsAdId
	$ip		$ip
	af_message		af_message
	androidDeviceId		androidDeviceId
api2.amplitude.com 18 peticiones	session_id	api2.amplitude.com 12 peticiones	session_id
	información del dispositivo (device_brand, device_manufacturer,)		información del dispositivo (device_brand, device_manufacturer,)
	limit_ad_tracking		limit_ad_tracking
	gps_enabled		gps_enabled
	user_properties		user_properties
	user_id		user_id
	device_id		device_id
	af_status		af_status
	información general del dispositivo y cuenta		información general del dispositivo y cuenta

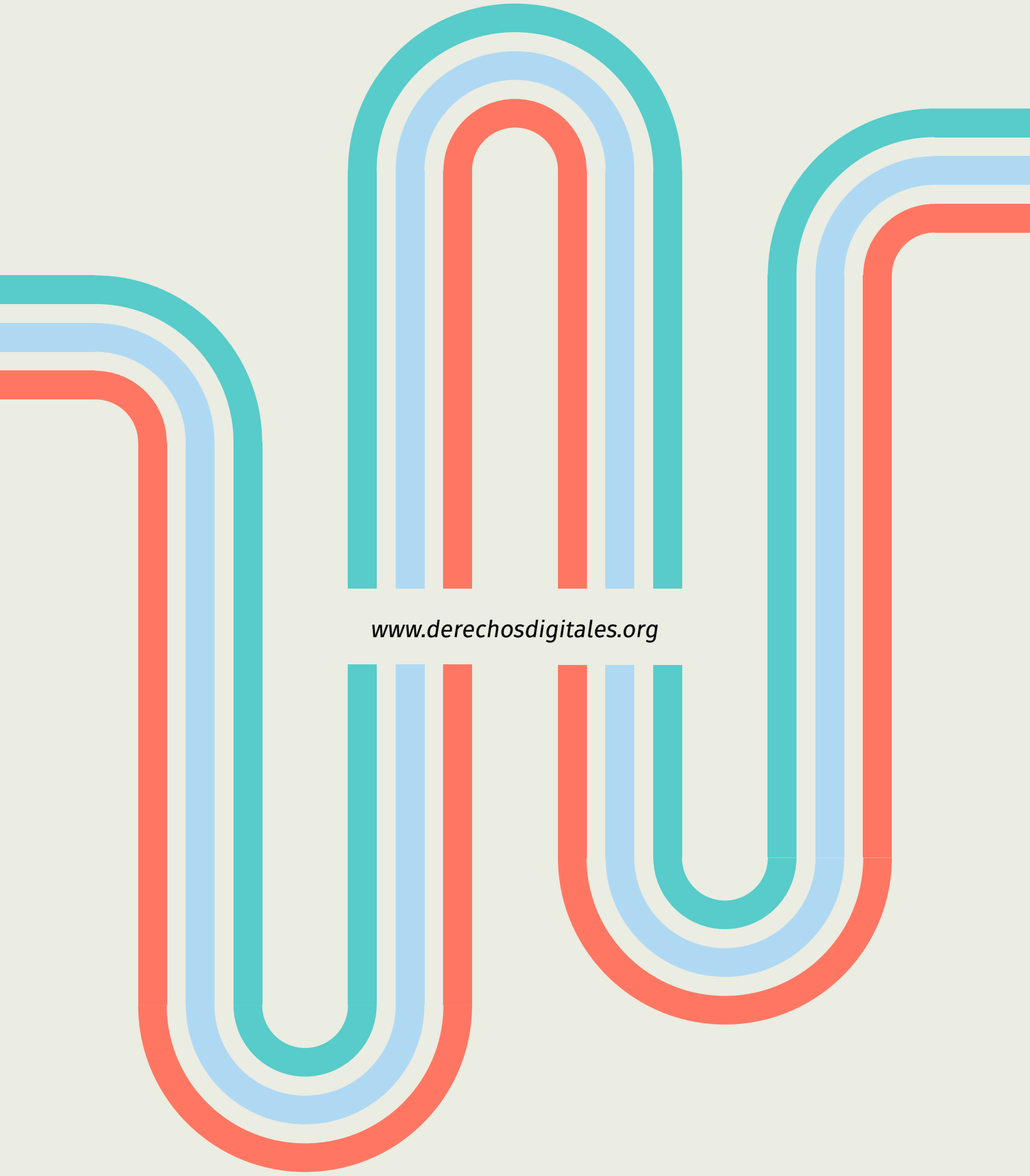
CONCLUSIONES

Tras realizar el análisis, una primera cuestión que salta a la vista es que, a pesar de la disparidad entre los regímenes de protección de datos personales entre Chile y Uruguay, no fue posible encontrar diferencias sustantivas respecto al funcionamiento de los rastreadores en ambos países. Dado que Uruguay cuenta con un estándar muchísimos más alto que Chile en materia de protección de datos personales, hubiésemos esperado que la recolección de información hubiese sido menor en el caso de las pruebas realizadas en este país. Tal como mencionamos anteriormente, el resultado de este ejercicio de investigación no pretende constituirse como prueba definitiva del mérito de una normativa y se requiere proseguir con la investigación, tanto a nivel técnico como legal, para poder comprender las posibilidades que el marco jurídico uruguayo otorga para la protección de los datos de las personas que allí habitan frente a este tipo de prácticas.

A partir del resultado, levantamos la hipótesis de que los marcos normativos no son capaces por sí mismos de prevenir prácticas potencialmente violatorias de derechos, sino que requieren estar dotadas de una institucionalidad proactiva y la colaboración de una ciudadanía empoderada que exija cada vez mayores niveles de protección. Esta puede ser una lección particularmente interesante para los países como Chile y otros de la región que están mejorando sus regulaciones.

En relación con las aplicaciones, preocupa tanto la cantidad de información que recolectan, como el hecho de que las empresas que las administran no transparenten la presencia de rastreadores ni los datos que comparten con cada uno de ellos. Esto es doblemente alarmante en el caso de aplicaciones como Fitia y Fastin Tracker, que declaran no compartir información con otras empresas u organizaciones, lo cual es falso.

Por último, no deja de llamar la atención la ubicuidad de los rastreadores de Meta/Facebook y Google. El nivel de información que estas compañías recaban de las personas a partir de las más variadas fuentes debe ser entendida no solamente como una afrenta contra el derecho a la privacidad y a la protección de los datos de las personas —más todavía cuando estas actividades se realizan sin conocimiento de los titulares de dicha información— sino también como una forma de extractivismo que erosiona las nociones de autonomía, intimidad y libertad, tanto a nivel personal como colectivo, en tanto se constituye un abierto desafío a la capacidad de los Estados para poner freno a este tipo de prácticas y proteger íntegramente la vida de sus ciudadanos.


www.derechosdigitales.org