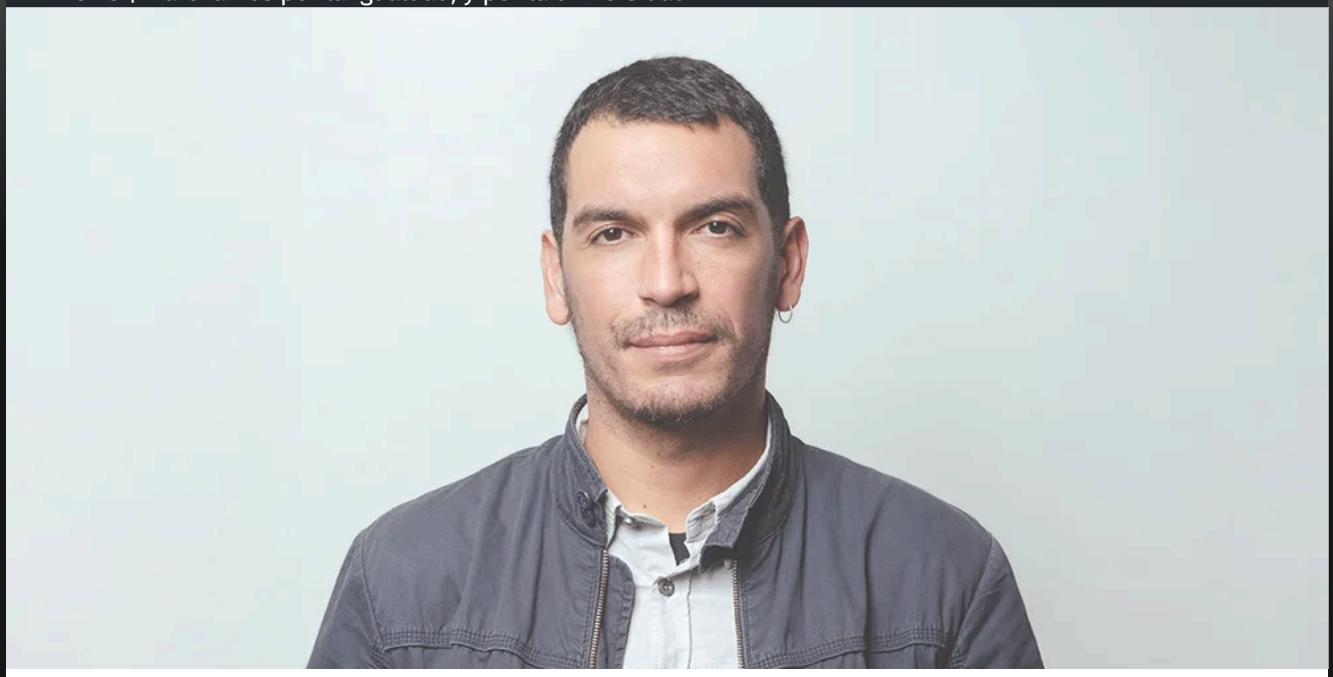
ISSN 2524-9290

bordes
Revista de Política, Derecho y Sociedad
UNPAZ
Universidad Nacional de José C. Paz

<- Previo | Marchamos por la igualdad, y por la universidad



SEGURIDAD DIGITAL

“ESTAMOS RODEADOS DE CÁMARAS POR TODOS LADOS Y ESA ADMINISTRACIÓN QUEDA EN MANOS DE NADIE”

14 mayo, 2026 Entrevistas

Entrevista a Miguel Flores, especialista en seguridad digital

Miguel Flores es director de Tecnologías en Derechos Digitales, una organización que lleva 20 años trabajando Derechos Humanos en entornos digitales en el contexto del siglo XXI. Es Ingeniero de sistemas y desarrollador, estudió Ingeniería en la Universidad Técnica Federico Santa María (Chile). Como experto en seguridad digital tiene más de 15 años de experiencia en el sector público, privado y de la sociedad civil. Flores sostiene que “la vigilancia masiva es un problema

 ISSN 2524-9290

actual en América Latina" y que es necesario visibilizar el colonialismo de datos.

Bordes: En Latinoamérica miramos el conflicto de Estados Unidos e Israel con Irán a cierta distancia –con la certeza que tendrá impacto sobre nuestras economías–, pero fuera del alcance de bombas y misiles. En un artículo reciente[1], hacés foco en otras armas no tan visibles, como el hackeo de las cámaras de seguridad, cámaras civiles, de tránsito, urbanas. ¿Podés explicar qué es lo que se sabe, qué trascendió? Y ¿por qué nosotros, desde nuestra región deberíamos prestar atención a esto?

Miguel Flores: Cuando ejecutan al Ayatolá se empiezan a esparcir una serie de noticias que tienen relación con la intervención de cámaras de seguridad[2], tanto las que están puestas en lugares públicos, como cámaras de tráfico; o videovigilancia que están en lugares cerrados. Técnicamente es muy viable. No es algo que esté sacado de una película. Y eso tiene que ver principalmente porque las cámaras en general, y muchos otros dispositivos operan con un sistema operativo, o firmware se llaman cuando son más pequeñitos; y esos sistemas –así como muchas otras cosas– presentan vulnerabilidades, sobre todo cuando están desactualizados. Pongo el ejemplo más conocido, cuando se desactualiza el Windows es más fácil que entre un virus. Entonces, la misma idea cabe para este tipo de dispositivos.

B: ¿Y cómo es que lo pudieron hacer? ¿Lo hicieron en un momento? ¿Lo venían haciendo hace tiempo? ¿No se detectó?

MF: Es plausible pensar que ya lo venían haciendo hace tiempo, y contaban con la tecnología y quizás el mapeo de las cámaras. Entonces, cuando necesitaron hacer uso de ellas, simplemente accedieron. Esto tiene que ver con las vulnerabilidades que pueden estar presentes en un sistema desactualizado, pero aparte de eso, Israel cuenta con una vasta envergadura de empresas que trabajan a nivel de tecnología y de seguridad ofensiva. Es decir, puede ser que hayan desarrollado tecnología específica para atacar cámaras, algo que no es público. No lo podemos ver, pero tiene una gran industria de seguridad digital detrás.

B: ¿Qué es lo que nosotros deberíamos pensar desde América Latina, teniendo presente nuestro grado de dependencia tecnológica, y los sistemas de software que usamos?

 ISSN 2524-9290

MF: Primero, es importante entender que como países latinoamericanos no tenemos la capacidad de producción de hardware de los dispositivos electrónicos: por la división global de trabajo y porque la competencia y la inversión serían muy muy grandes para algún Estado. Entonces, eso ya genera una brecha en términos de qué capacidad tienen los Estados para poder controlar infraestructura que podría llamarse estratégica. O sea, tener control sobre cámaras de seguridad en vías públicas, en puertos, hospitales o cualquier tipo de lugar que pueda resultar estratégico, ya sea para un conflicto armado o no. En ese sentido es difícil pensar en solucionar ese problema de un día para otro. Porque producir hardware podría costar un par de años, sino décadas.

Entonces, la reflexión que hacemos nosotros es que, si bien eso no se ve viable al corto o mediano plazo, el control del software sí permitiría tener algún nivel de independencia, en términos no solo de los hackeos, sino también de aquellos requerimientos que puedan estar presentados por los gobiernos donde residen las empresas que producen estos dispositivos.

B: ¿Qué quiere decir esto?

MF: Sirve como ejemplo la última discusión que tuvo la empresa Anthropic con el Pentágono. El Pentágono quería acceder a una mayor funcionalidad del motor de inteligencia artificial con fines armamentísticos o de vigilancia masiva. Ese tipo de discusiones o concesiones nos hacen reflexionar respecto de qué sucede con otros elementos de la tecnología, y si estos también en algún momento pueden o tienen que responder a los Estados donde las empresas fueron creadas o están radicadas.

B: ¿Hay algún indicio de que alguna vez se hayan hackeado las cámaras públicas o privadas de una ciudad latinoamericana?

Primero, las personas encargadas de esas cámaras poseen equipos técnicos, y personal que debiese ser el encargado de revisar que las cámaras no hayan sido vulneradas. Porque tienen el acceso directo a la administración y ellos pueden revisar y ver si algo pasó. Pero sí, sucede que, más allá de eso, las cámaras no solo son del gobierno o del Estado. Hay un montón de cámaras que la gente coloca, estamos rodeados de cámaras por todos lados y esa administración queda en manos de nadie. Porque la instala un técnico, y viene con una versión de su

 ISSN 2524-9290

sistema, pero pasan dos o tres años y ese sistema está obsoleto. Entonces, la cámara queda vulnerable a ataques y a que alguien pueda tomar control de ella.

B: ¿Y cómo se podría resolver esa situación, que una cámara no quede desactualizada y vulnerable como una mirilla para un enemigo?

MF: En ese sentido para lo que es la población en general es muy difícil, porque la gente compra las cámaras, las instala y ahí quedan. Pero sí quizás el debate es más a nivel de Estados. Hacemos una separación lógica entre dos tipos de cuestiones, lo que es la construcción del hardware y lo que es el manejo del software, con el sistema operativo que tienen estas cámaras. Y en ese sentido, una forma de minimizar esta brecha de seguridad podría ser el uso de software libre, por razones como que el código fuente de las aplicaciones de código abierto es libre y públicamente accesible y auditable. Entonces es muy poco probable que existan vulnerabilidades por diseño. Es decir, que hayan colocado una función que en caso de ser necesaria sea activada. Es muy difícil porque es auditable públicamente.

Por otro lado, al ser código abierto también se pueden modificar funciones y entonces uno puede decir, “Bueno, esto no lo voy a necesitar” y quitar esa parte de código. Y, por último, que la actualización sea gratuita permite actualizarla en cualquier momento. Lo que sucede más comúnmente es el uso de software privativo, que viene junto con esas cámaras por lo general. Entonces, los problemas pasan porque el código es cerrado y no es audible. No sabemos todas las funciones que pueda tener ese software. Y, además, como son software pagos, si las actualizaciones no se ejecutan, ese sistema queda vulnerable.

B: ¿Te resultan plausibles estas versiones que dicen que los líderes, las autoridades iraníes tenían dificultades para coordinar acciones, que no querían comunicarse por el temor a ser geolocalizados con precisión a través de sus teléfonos? ¿Qué riesgo ves que podría técnicamente haber en los teléfonos?

MF: Claro, es plausible en un sistema de inteligencia. Hay una gran industria detrás del desarrollo de programas para vulnerar teléfonos, porque contienen mucha información importante. Y si eso lo interseccionamos con cámaras, satélites, otro tipo de tecnología, muchas otras cosas, claro que pueden geolocalizar y dar con alguien. Es

 ISSN 2524-9290

muy plausible poder hacerse con un aparato de inteligencia de un Estado.

B: Decís que la gente pone una cámara, la instala y después se olvida y no se da cuenta el riesgo que puede haber ahí. En una entrevista a Eric Sadin, el filósofo francés, decía que "las sociedades en cuestiones digitales se despiertan siempre demasiado tarde" ¿Crees que es un poco así?

MF: Yo creo que la tecnología nos parece maravillosa y abrumadora por las cosas que hace, pero me parece preocupante que no somos capaces de prever el impacto que puede tener en nuestra vida cotidiana, en nuestra interacción social.

B: Porque por lo que describís en el artículo, el estar rodeados de aparatos que tenemos conectados, el internet de las cosas, a través de los que nos podrían espiar, puede generar una sensación de mayor inseguridad. ¿Qué es un refugio hoy en el siglo XXI en un mundo en conflicto?

MF: A partir del ejemplo de las cámaras de seguridad me atrevería a decir que también es plausible pensar que hay muchos otros sistemas que pueden ser vulnerados. Entonces, va a depender también de qué es lo que uno cree que es privado o no, el tipo de tecnología que quiera o pueda usar en su casa. Es un poco preocupante como de pronto la gente cada vez usa más dispositivos automatizados y conectados a internet y cómo eso puede afectar su privacidad. No se ve en el día a día, porque uno hace cosas cotidianas, pero quién sabe si en un futuro no puede ser un arma de doble filo.

B: ¿Qué te parece que han sido los mayores avances o retrocesos en la agenda de los derechos digitales, que no es una agenda que esté muy alta en la conversación pública?

MF: Coincido en que como algunos elementos son técnicos, ya sea de índole digital y/o técnicos-legales resulta difícil bajarlos a un lenguaje cotidiano .Pero, por ejemplo, como avances podríamos mencionar, algunas actualizaciones legislativas en algunos países de América, en Chile 2026, Paraguay 2025, en las cuales se hace una traducción o una

 ISSN 2524-9290

adaptación de la de la GDPR (por sus siglas en inglés) la Ley de Protección de Datos de Europa para poder también cubrir y asegurar un mejor entorno para los datos de las personas de Latinoamérica.
También se ha buscado hacer adaptaciones de las IAs. Los grandes motores provienen del norte global y de la big tech, de las grandes empresas de tecnología, y, entonces, se ha cuestionado el hecho de no tener motores propios, que se alimenten de historias y lenguajes propios de nuestro continente. Y en términos de retrocesos, la vigilancia masiva es un problema actual en Latinoamérica.

B: Hablabas de la IA. Desde Argentina se promociona lo de instalar data centers, como la llegada de la IA, dejando un espacio de ambiguedad o confusión entre ser un territorio de computo y el desarrollo local. ¿Pensás que hablar de dependencia/independencia tecnológica viene un poco trastocado por distintas narrativas?

MF: La llegada de data centers de las grandes empresas de tecnologías a Latinoamérica responde en gran parte a necesidades propias de las empresas que necesitan distribuir sus datos en distintos lugares para replicarlos o tener una vía más rápida donde almacenar, pero les siguen perteneciendo. Están dentro de sus servidores, dentro de sus computadoras. Un tema a discutir es el colonialismo de datos, cómo las grandes empresas obtienen datos de nosotros a través de los gobiernos u otras formas. Es preocupante, dado lo que mencionaba anteriormente, como otro Estado extranjero tiene acceso a tanta información sobre otro Estado, el cual le puede servir en algún momento en alguna negociación o conflicto. Desde Derechos Digitales creemos que es fundamental pensar en esto. Y vemos poco movimiento hacia pensar la tecnología como un bastión de independencia en la región. Ha pasado por temporadas, va variando según gobiernos, pero no hay una estrategia regional común o países que tengan una línea conductora que se puede ver a través del tiempo.

B: ¿Qué es el colonialismo de datos?

MF: Lo voy a ejemplificar para que se entienda mejor. Los modelos de lenguaje o lo que nosotros comúnmente llamamos modelos de IA se alimentan de datos para poder entender cómo funcionan nuestras respuestas e imitar como respuestas humanas. Y para eso necesitan muchos datos, millones de datos, volúmenes muy grandes de datos. Entonces, eso que antes parecía una cosa, o sea, guardar un número de teléfono para tener el contacto o guardar el correo para poder enviar spam, o publicidad o lo que fuera, ahora ya tiene otro cariz, que

 ISSN 2524-9290

consiste en acumular datos, para poder analizarlos a través de estos motores y poder generar modelos predictivos de cómo sería lo que una persona o cierta sociedad o cierto grupo pudiera pensar en determinada situación. Entonces, las grandes empresas tecnológicas que desarrollan estos modelos están en el norte global.

En latinoamericana estamos subyugados culturalmente a usar ciertas aplicaciones. Quiero decir, el mapa de influencia de ciertas redes sociales que nosotros utilizamos están en Europa y Sudamérica. Asia e India usan otras aplicaciones. Es decir, lo que nosotros llamamos redes sociales que es Instagram, WhatsApp y Facebook son válidas en ciertos territorios, no en todo el mundo. Esas empresas, se benefician de todos nuestros datos. Entonces, otorgan una mayor ventaja nuevamente al norte global.

[1] Flores, M. (2026). *La guerra por otros medios: control de software e infraestructura estratégica.*

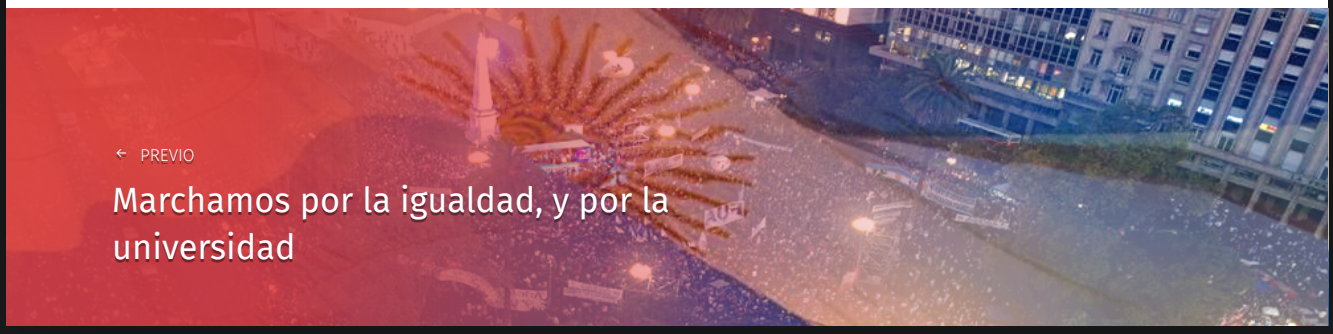
Recuperado de https://www.derechosdigitales.org/recursos/la-guerra-por-otros-medios-control-de-software-e-infraestructura-estrategica/

[2] Shalev, T y Diamond, J. (4-3-2026). *Hacked traffic cameras and US intelligence: How a plot to kill Iran's supreme leader came together.* Recuperado de

https://edition.cnn.com/2026/03/03/middleeast/us-israel-plot-kill-iran-khamenei-latam-intl

Comentarios:

#seguridad digital



PREVIO
Marchamos por la igualdad, y por la universidad

Universidad Nacional de José C. Paz

Leandro N. Alem 4731, José C. Paz,
Pcia. de Buenos Aires (CP 1665)
http://www.unpaz.edu.ar
Email: revistabordes@unpaz.edu.ar

Revista Bordes
ISSN 2524-9290

Etiquetas

24 de Marzo
40 años de democracia
2001
alimentación
Chile
COVID-19
democracia
derechos
derechos humanos
desaparecidos
Dictadura Militar
drogas
Día del Trabajador
ecología
Ecuador
Educación
elecciones
estado
feminismo
FEMINISMOS
filosofía
fútbol
golpe de estado
género
historia
Horacio González
Iglesia
igualdad de género
Inteligencia artificial
juicio a las juntas militares
Julio Cortázar
literatura
medio ambiente
Migraciones
Milei
neoliberalismo
pandemia
política

Buscador

Escriba la palabra buscada y pre

ISSN 2524-9290

que se vayan todes
redes sociales
salud
sistema carcelario
Trabajo
trimestrales
Universidades

 Regresar arriba ↑