VIGILANCIA MASIVA EN EL MAGHREB Y EL MASHREQ

Un análisis crítico para proteger el espacio de la sociedad civil

RESUMEN EJECUTIVO

En las últimas décadas, el desarrollo tecnológico y la digitalización han facilitado la aparición de nuevas técnicas de vigilancia y control cada vez más extendidas e intrusivas, que plantean nuevos retos en la protección de los derechos humanos. Este informe analiza cómo los gobiernos y empresas en la región del Maghreb y Mashreq utilizan tecnologías avanzadas de vigilancia digital para controlar y reprimir a la sociedad civil, afectando de forma diferencial a personas migrantes, mujeres y comunidad LGBTIQ+. Estas tecnologías, desarrolladas en gran parte por empresas del norte global, han creado un contexto de vigilancia masiva que amenaza derechos fundamentales como la libertad de expresión, la privacidad y el derecho a la información. Las tecnologías emergentes se adquieren con el argumento de mejorar la seguridad nacional y bajo pretextos de adaptación a nuevas formas de criminalidad, pero restringen el espacio de participación política y aumentan el control social.

Este informe complementa el anterior publicado centrado en el uso de la tecnología de vigilancia masiva en Europa. La combinación de ambos informes proporciona una visión del uso de estas tecnologías y su impacto en la sociedad civil de la región Mediterránea.

El informe realiza un análisis especifico de la situación en 9 países de la región:

- **Marruecos**: La represión digital en Marruecos incluye el uso de spyware como Pegasus, y el *trolling online* utilizados para difamar y acosar a figuras críticas con el sistema. Se vulnera especialmente los derechos de las mujeres activistas y periodistas, que sufren campañas de desprestigio con connotaciones misóginas. Esta represión es respaldada por una legislación opaca y tecnologías intrusivas suministradas por empresas del norte global.
- **Sáhara Occidental**: Desde el fin de la tregua en 2020, la represión y vigilancia sobre la población saharaui se han intensificado. Con el respaldo de tecnología avanzada, incluida la colaboración militar con Israel y la implementación de drones y sistemas de vigilancia digital, Marruecos ha impuesto un control severo en el Sáhara Occidental. Esto afecta tanto a defensoras de derechos humanos como a periodistas saharauis, especialmente a mujeres. Esta estrategia ha creado un clima de represión sistemática, forzando el desplazamiento de la población civil y afectando derechos fundamentales de movimiento, privacidad y expresión, con el objetivo de consolidar

su control sobre el territorio ocupado.

- **Túnez**: En estado de emergencia permanente, Túnez mantiene prácticas de vigilancia heredadas de la dictadura para controlar a activistas, juezas, periodistas y personas LGBTIQ+, usando leyes de ciberdelincuencia que permiten la recopilación de datos privados y el hackeo de dispositivos. Mediante la Ley de Ciberdelincuencia, más de 40 personas han sido detenidas por su activismo, mientras que la vigilancia fronteriza con Libia, financiada por el norte global, endurece la represión contra personas migrantes y refuerza el control estatal.
- **Egipto:** El gobierno egipcio emplea una red de ciberespionaje avanzada, utilizando spyware como *Cytrox's Predator* y tecnología de censura como la inspección profunda de paquetes (DPI) para interceptar comunicaciones. También ha bloqueado más de 600 sitios web críticos con el régimen. La represión digital incluye campañas de acoso y difamación en redes sociales dirigidas a activistas, periodistas y defensoras de derechos humanos, apoyadas por bots y cuentas progobierno, con ataques homófobos y misóginos frecuentes.
- **Líbano:** Las agencias de inteligencia llevan a cabo un monitoreo exhaustivo de las comunicaciones de la sociedad civil, utilizando tecnologías avanzadas como el sistema de ciberespionaje *Dark Caracal*. La infraestructura digital en el Líbano es vulnerable, siendo la mayor brecha de seguridad en el país el reciente ataque masivo de Israel dirigido contra militantes de Hezbollah a través de la explosión de sus dispositivos, buscas y walkie-talkies. La Oficina de Ciberdelincuencia sirve para silenciar a periodistas, activistas y blogueras mediante el uso de leyes restrictivas, lo que fomenta la autocensura y el cierre de contenidos digitales.
- **Siria:** El ciberespacio en Siria está fuertemente regulado y controlado mediante nuevas legislaciones que avalan prácticas represivas para criminalizar la libertad de expresión y el libre flujo de información. El gobierno utiliza diversas unidades de su aparato de seguridad para monitorear comunicaciones y regular el acceso a internet. Desde la Primavera Árabe, ha incrementado su control, incluyendo la detención de activistas y la imposición de penas severas por difundir "fake news". Además, se emplean "ejércitos electrónicos" y grupos de hackers para perseguir y vigilar a opositoras tanto dentro como fuera del país. La represión es particularmente intensa contra la población kurda, que enfrenta violaciones de su derecho de reunión y libertad de expresión.
- **Palestina:** La ocupación israelí de Gaza y Cisjordania ha permitido la experimentación y el desarrollo de tecnologías de vigilancia, consagrando a Israel como líder mundial en este ámbito. Esta colaboración entre el Estado y empresas de ciberseguridad es fundamental para sostener el sistema de apartheid que sufre la población palestina. Las herramientas de represión digital incluyen el monitoreo de defensoras de derechos humanos en redes sociales y el uso de apagones de Internet como castigo colectivo. El genocidio actual en Gaza ha intensificado estas violaciones de derechos, introduciendo el uso de inteligencia artificial para aumentar la letalidad de los ataques. A través de tecnologías avanzadas, como sistemas de reconocimiento facial y armas autónomas, Israel ha escalado su control y vigilancia sobre las palestinas, exacerbando

la crisis humanitaria y la represión en la región.

- **Jordania:** La censura digital en Jordania ha aumentado significativamente en los últimos años, afectando principalmente a activistas LGBTIQ+ y periodistas. El gobierno utiliza la Ley de Ciberdelincuencia para intimidar y perseguir a periodistas, lo que ha llevado al cierre de numerosos sitios web independientes. En particular, durante las recientes manifestaciones en la capital jordana, que se intensificaron tras el genocidio en Gaza, se han instalado miles de cámaras de vigilancia para controlar y documentar las protestas, identificando a las participantes.
- **Irak:** La censura de contenido digital y el acoso online perpetrados por ejércitos electrónicos en Irak afectan gravemente a mujeres y la comunidad LGBTIQ+. Estos ataques en línea a menudo preceden a ataques físicos. Irak es líder en la región en el uso de apagones digitales, que se utilizan especialmente durante movilizaciones y protestas sociales. Desde 2019, el gobierno ha bloqueado el acceso a internet en 126 ocasiones, lo que ha contribuido a la violencia contra activistas al dificultar la difusión de información sobre abusos.

Las principales tendencias de vigilancia masiva identificadas en la región son:

1. **Aumento del autoritarismo y represión de las disidencias:** Gobiernos de la región han expandido sus capacidades de control sobre la sociedad civil, limitando el flujo de información y la capacidad de movilización de los movimientos sociales. Este proceso se ha reforzado desde las Primaveras Árabes mediante el uso de tecnologías que permiten el monitoreo de la población y el control de las comunicaciones.
2. **Participación de empresas internacionales en el desarrollo de tecnologías represivas:** Empresas de Israel, Estados Unidos y Europa han suministrado tecnologías de vigilancia y control que los gobiernos de la región utilizan para reprimir a las disidencias y espiar a defensoras de derechos humanos y periodistas. Esta represión es más grave en los territorios ocupados.
3. **Uso de spyware y ciberespionaje:** En países como Marruecos y Egipto, el uso de software espía como Pegasus permite la vigilancia de dispositivos de personas y organizaciones críticas con el régimen. Estas tecnologías posibilitan el acoso digital y la recolección de información privada para atacar la reputación de activistas, periodistas y defensoras de derechos humanos, limitando el espacio para el activismo y la libertad de expresión.
4. **Estrategias de control en redes sociales:** Para controlar la opinión pública se realizan campañas de desinformación y manipulación en redes sociales, mediante cuentas falsas que difunden contenido afín al régimen y difaman figuras de oposición. En el caso de la población LGBTIQ+ y las mujeres defensoras, se ha detectado un acoso diferencial que frecuentemente usa información privada para difamarlas y desacreditarlas. En algunos contextos como Irak y Marruecos, se ha identificado también cómo estas estrategias buscan hacer cómplice a la población en general, que lleva el acoso iniciado en las redes en un ámbito público.

5. **Apagones de internet.** Ante el potencial organizativo de las nuevas tecnologías de la información y redes sociales, se ha identificado una estrategia de "desconexión" que se utiliza para prevenir la organización y denuncia de los movimientos sociales. Se ha observado como estos bloqueos aumentan la represión policial. En Irak, Palestina y Siria esta práctica es frecuente.

Conclusiones clave:

1. **Erosión del espacio cívico:** La vigilancia masiva en la región mediterránea limita significativamente la libertad de expresión, la capacidad de organización y la defensa de los derechos humanos al generar un clima de represión que provoca, entre otros efectos, la autocensura.
2. **Complicidad internacional:** Los gobiernos del norte global y empresas de estos países han contribuido al desarrollo y la exportación de tecnologías de vigilancia sin mecanismos efectivos de rendición de cuentas, lo que perpetúa la impunidad en las violaciones a los derechos humanos.
3. **Afectación diferencial a colectivos vulnerabilizados:** Mujeres, comunidad LGBTIQ+, personas migrantes y defensoras de derechos humanos son las más afectadas, enfrentando no solo vigilancia, sino acoso digital y amenazas específicas.
4. **El rol de la ocupación en el ecosistema de la vigilancia masiva:** Gran parte de las tecnologías identificadas se desarrollan y testean sobre el pueblo palestino que vive bajo ocupación militar israelí. Mientras, Marruecos se ha convertido en un actor clave en el desarrollo del sector en la región, impactando gravemente en los derechos del pueblo saharaui. Las ocupaciones, y el genocidio, son factores que benefician al ecosistema empresarial de la vigilancia.
5. **Necesidad urgente de regulación:** La falta de normativas específicas y de marcos legales que regulen el uso de la vigilancia masiva permite a los gobiernos abusar de estas tecnologías en nombre de la seguridad nacional y la lucha antiterrorista. Los mecanismos de protección son ineficaces, lo que dificulta que las víctimas de esta vigilancia encuentren justicia y reparación.

Observatori de Drets Humans i Empreses · NOVACT · suds Internacionalisme Solidaritat Feminismes · Irídia · Al-Himaya Defensa de l'espai cívic a l'euromediterrània