VIGILANCIA MASIVA EN EL MAGHREB Y EL MASHREQ

Un análisis crítico para proteger el espacio de la sociedad civil

---

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

VIGILANCIA MASIVA EN EL MAGHREB Y EL MASHREQ

Un análisis crítico para proteger el espacio de la sociedad civil

Noviembre 2024

Autoras principales: Dúnia Camps-Febrer, Felip Daza, Carlos Díaz y Nora Miralles

Autoras contribuyentes: Berta Flores y Paula Mas

Coordinación: Maite Ramos Plaza [maite@suds.cat] y Alys Samson Estapé [alys@novact.org]

Comunicación: Lucrecia Baquero Ramos (Observatorio de Derechos Humanos y Empresas en el Mediterráneo), Julia Ponti Estrems (NOVACT), Ionan Areses (SUDS)

Asistencia legal: Laia Serra Perelló

Maquetación: Carmela Márquez B @edicionescaseras

Traducción: Lia Giralt

El Observatorio de Derechos humanos y Empresas en el Mediterráneo (ODHE) es una iniciativa conjunta de NOVACT y SUDS.

Agradecemos a una serie de personas que generosamente han ofrecido su ayuda: Itxaso Domínguez de Olazábal, Ahmed Ali, Omar Alaameri, Anabel Karina Arias, así como a todas las defensoras de derechos humanos que han contribuido en la investigación y a todo el equipo de SUDS y NOVACT.

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

Informe realizado en el marco del proyecto:
Alhimaya – Defensa del espacio cívico y protección de defensoras en el Euromediterráneo.

Con el apoyo de:

Agència Catalana de Cooperació al Desenvolupament · Generalitat de Catalunya

ÍNDICE

ACLARACIONES SOBRE TERMINOLOGÍA EMPLEADA:

El derecho internacional considera el territorio palestino de Cisjordania, incluyendo Jerusalén Este, y la Franja de Gaza, ilegalmente ocupado por Israel. Otras autoras consideran que toda la Palestina histórica – el área colonizada bajo el protectorado británico de 1918 a 1948 – es un territorio ocupado puesto que el Estado de Israel se creó a partir de la expulsión de gran parte de la población autóctona que vivía en él, el pueblo palestino. En este informe cuando hablamos de Territorio Ocupado Palestino (TOP) nos referimos a la Franja de Gaza, y/o Cisjordania, incluyendo Jerusalén Este.

Naciones Unidas considera el Sahara Occidental como un territorio no autónomo, cuyo proceso de descolonización está sujeto al referéndum de autodeterminación previsto por el Plan de Paz de 1991. En este contexto, España es la potencia administradora, mientras que Marruecos es considerada potencia ocupante. Para la Unión Africana y más de medio centenar de Estados, el Sahara Occidental, es la República Árabe Saharaui Democrática, un estado soberano. En este informe cuando hablamos de territorio ocupado del Sáhara Occidental nos referimos a la República Árabe Saharaui Democrática.

Además, en este informe, en general, utilizaremos el femenino genérico como expresión lingüística referida a personas.

PRÓLOGO

El uso indiscriminado de la vigilancia masiva por parte de Estados y empresas está poniendo en peligro los fundamentos de las democracias a nivel global.

Las nuevas tecnologías están proporcionando a los Gobiernos herramientas cada vez más potentes para controlar a movimientos sociales, medios de comunicación y disidencia en general. El sector tecnológico y el comercio de la vigilancia actúan en un contexto prácticamente libre de regulaciones, convirtiéndose en una pieza clave de la arquitectura represiva. Esto ha llevado a la normalización de prácticas ilegales por parte de algunos estados, que utilizan estas herramientas para perpetuar el control y la represión. Es en ese contexto donde irrumpe la inteligencia artificial, elevando aún más las dinámicas de discriminación. Además, las regulaciones que se crean carecen de enfoque extraterritorial y se salvaguardan en la seguridad nacional para incorporar excepciones. En septiembre de 2021, la Alta Comisionada para los Derechos Humanos de Naciones Unidas pidió una "moratoria urgente en la venta y el uso de la inteligencia artificial" y las tecnologías asociadas; y según el propio Relator de Naciones Unidas para la Libertad de Expresión, la implementación de mecanismos de vigilancia y control está afectando al derecho a la libertad de expresión, opinión y privacidad con profundas vulneraciones contra las personas defensoras de derechos humanos y periodistas.

Los mecanismos de vigilancia y control erosionan gravemente derechos fundamentales como la libertad de expresión, de opinión y de privacidad, con un impacto especialmente duro sobre las personas defensoras de derechos humanos y las periodistas, a menudo objetivo directo de estas prácticas de acoso.

Este informe es una continuación de nuestro estudio "Mass Surveillance y control de la disidencia en Europa" (2021), donde ya alertábamos sobre el uso de estas tecnologías por parte de Gobiernos europeos. Ahora ampliamos nuestra mirada hacia el Maghreb y el Mashreq, dos regiones donde hay un claro patrón: empresas del norte global —mayoritariamente europeas, estadounidenses e israelíes— desarrollan tecnología a menudo "testada en combate" en contextos de graves vulneraciones de derechos humanos, especialmente en territorios ocupados. Esta tecnología es adquirida posteriormente por regímenes cada vez más autoritarios con el objetivo de reprimir a las disidencias y movimientos sociales. Así, el ascenso del autoritarismo está sustentado en un entramado de organizaciones, empresas e instituciones que legitiman un orden social de opresión, basado en el abuso del poder estatal y empresarial, la polarización social y el uso de la violencia en sus diversas formas.

Desde Marruecos hasta Irak, los Gobiernos y las empresas privadas de la región están desplegando herramientas de vigilancia digital cada vez más sofisticadas para identificar, monitorear y silenciar a las disidencias, periodistas, defensoras de derechos humanos y activistas feministas y medioambientales. Muchos de estos Gobiernos cuentan con el apoyo del norte global, quien avala estas prácticas represivas con el objetivo de sofocar cualquier amenaza al statu quo. Así pues, existe una interdependencia entre el desarrollo y uso de las tecnologías de vigilancia, y un contexto global de impunidad empresarial.

Este informe quiere visibilizar esta relación, con el objetivo de identificar y comprender las tendencias que el autoritarismo pone en práctica a nivel global, pero también sus especificidades en el ámbito local.

Actualmente, la región mediterránea experimenta una severa limitación del espacio cívico, indispensable para el ejercicio y defensa de derechos fundamentales como la libertad de expresión, de asociación y de reunión. Estos derechos son cruciales para garantizar una interacción libre y segura entre la sociedad civil y los Gobiernos, sin miedo a represalias. Viendo cómo la tecnología está generando las capacidades para tener bajo control a la disidencia, nos inquieta qué futuro tienen las democracias. Los derechos que se han logrado a lo largo de la historia no han sido concedidos, sino conquistados gracias a las luchas sociales. Es altamente preocupante que los estados tengan cada vez más herramientas para monitorear, perseguir y silenciar a los movimientos sociales y de defensa de derechos humanos, poniendo así en riesgo muchos de los derechos que tanto ha costado conseguir.

Esta degradación democrática restringe la capacidad de la sociedad civil para autoorganizarse, implicarse en la vida pública y erigirse como defensora de los derechos humanos, con un impacto especialmente grave sobre aquellos colectivos más vulnerabilizados por sistemas de opresión basados categorías racistas, de género y de clase social.

Es en este contexto en el que expresamos nuestra preocupación sobre cómo las nuevas tecnologías están reforzando estas desigualdades, facilitando la vulneración sistemática de derechos y silenciando a las disidencias que luchan contra esta deriva autoritaria.

En este informe aportamos análisis y diagnosis de lo que está pasando, conocimientos del fenómeno y de los matices que se producen en diferentes contextos, con el fin de construir estrategias colectivas para revertirlo. También aportamos argumentos y herramientas para subrayar la necesidad urgente de regular estas tecnologías, que no sólo debilitan a las democracias, sino que también ponen en peligro la vida de las personas y los colectivos que trabajan para defenderlas. La carencia de mecanismos internacionales de regulación dificulta que las víctimas de la vigilancia selectiva encuentren justicia, reparación y garantías de no repetición. La creación de sistemas de control y regulación es imprescindible tanto a nivel estatal como supraestatal, tanto para las empresas que desarrollan estas tecnologías como para aquellas que las implementan y compran. En este sentido, queremos alertar a las administraciones sobre la urgente necesidad de establecer mecanismos de control y seguimiento que impidan la contratación pública de empresas y compra de tecnología vinculada a la vulneración de derechos humanos en toda la cadena de suministro. Es urgente recordar a los estados y empresas que es su responsabilidad velar por el respeto de los derechos humanos, y este informe es un paso más en esta dirección.

No queremos terminar sin mencionar la importancia de la creación de redes y estrategias de defensa de derechos humanos norte-sur que amplíen las perspectivas locales en un intercambio internacional basado en la reciprocidad. La interconexión, el intercambio de experiencias y la creación de alianzas son el motor de cambio y transformación para las entidades que promovemos esta investigación.

INTRODUCCIÓN

Las tecnologías de vigilancia y control, entendidas como el hardware y el software necesario para monitorear el comportamiento, las actividades y la información de la población, se han convertido en un lucrativo negocio que, en 2022, facturaba ya más de 130.000 millones de dólares y que se calcula supera ya los 150.000 millones a nivel global[1]. Un mercado controlado fundamentalmente por empresas occidentales, principalmente israelíes, centroeuropeas y estadounidenses, cuyos productos y tecnologías se aplican, como mostramos en este informe, de forma profusa y cada vez más extendida en los países del sur global.

Este desarrollo e inversión multimillonaria en herramientas de inteligencia artificial y tecnologías digitales para el control social sucede en un contexto global de auge del autoritarismo, del militarismo y de las vulneraciones de derechos humanos, en plena crisis ecológica y económica mundial de consecuencias todavía inciertas. Esta perspectiva es compartida por la enorme mayoría de las organizaciones de defensa de los derechos humanos y la democracia en el mundo. Amnistía Internacional advertía en 2019 de que "este giro autoritario global es existencial, amenaza a cada ser humano y a todas nuestras libertades, la igualdad y la justicia"[2].

El uso y acceso a las tecnologías digitales, sin embargo, también es diferenciado en función de las características de la población, destacando aspectos como la edad, el género o la división urbano-rural[3]. Todos estos factores determinan el impacto de las tecnologías digitales, tanto como vía de acceso o producción de información diversa, como vía de control o represión.

En el caso de la región mediterránea, y dentro de ésta en el Maghreb y el Mashreq, desde las Primaveras Árabes los regímenes han invertido en tecnologías de vigilancia masiva para controlar a la disidencia política. Sin embargo, el caso más extremo es la utilización de Israel del Territorio Ocupado Palestino (TOP) como laboratorio para el testeo de nuevas armas y tecnologías sobre la población civil, hecho que les ha permitido ser líderes mundiales en exportación de tecnologías de represión y control social. Una dinámica que se ha agravado enormemente desde el 7 de octubre de 2023. Tras el inicio del genocidio en Gaza, más de 41.000 personas palestinas han sido asesinadas por el ejército israelí en un contexto donde se han desplegado sistemas de inteligencia artificial extremadamente letales.

Estos ataques en Gaza han potenciado el uso y abuso de la vigilancia no solo contra la población palestina en el TOP, sino también contra la sociedad civil que se ha alzado en todo

---

1 **Statista.com**. "Surveillance Technology Market Size Worldwide from 2022 to 2027." Disponible en: https://www.statista.com/statistics/1251839/surveillance-technology-market-global/#:~:text=In%202022%2C%20the%20global%20surveillance,billion%20U.S.%20dollars%20by%202027.

2 **Amnesty International Norway.** Reflexión: "The Global Authoritarian Turn: Making Humanity Win." 2019. Disponible en: https://amnesty.no/sites/default/files/vedlegg/the_global_authoritarian_turn_-_making_humanity_win.pdf.

3 Ver datos desglosados por país en el Arab Barometer: **Arab Barometer.** "The MENA Digital Divide." Disponible en: https://www.arabbarometer.org/2020/09/the-mena-digital-divide/.

el mundo para denunciar las masacres y la inacción de la comunidad internacional. A ello se suma la desconexión digital forzada de la población libanesa en los pueblos y suburbios cuya infraestructura de comunicaciones ha sido bombardeada y destruida por Israel recientemente. Se han documentado, también en las zonas atacadas, mensajes intimidatorios y falsos llamamientos de evacuación a través de redes y aplicaciones de mensajería para confundir, intimidar y asustar a la población libanesa. Tendencias que, sin duda, dejan intuir otra vuelta de tuerca en el giro autoritario global y que merecen un análisis propio y urgente[4].

En este informe se analizan las tendencias y el rumbo que ha tomado, en los últimos años, la vigilancia masiva en el Maghreb y Mashreq, en continuidad con el proyecto de investigación "Vigilancia hi-tech en tiempos del COVID-19"[5] publicado por el ODHE en 2021, en el que ya se vislumbraban algunas de estas tendencias y empresas. Nuestro objetivo es facilitar la comprensión de cómo, en el despliegue de sus políticas de seguridad internas, la relación entre los Gobiernos y el sector empresarial tecnológico incide en la vulneración de los derechos humanos. La investigación sobre casos y productos se ha complementado con entrevistas a defensoras de derechos humanos que, en algunos casos, participaron en el encuentro "The Nonviolence Factory", organizado por NOVACT y celebrado en noviembre de 2023 en Barcelona, así como en el "Seminario Al-Himaya en defensa y protección del espacio cívico ante la vigilancia masiva en el Euromediterráneo", organizado por SUDS, NOVACT e Irídia en mayo de 2024.

Para ello, es básico comprender cómo se han desarrollado y probado estas tecnologías y las implicaciones sociales y políticas del uso de estas herramientas desde una perspectiva de derechos humanos. Desenmascarar la cadena global de la represión y el control social con un enfoque interseccional puede servir para reforzar la protección, movilización y trabajo de comunicación e incidencia de los grupos y colectivos afectados por estas vulneraciones, así como establecer alianzas entre defensoras de derechos humanos de diferentes territorios.

Conscientes de que nuestra posición y herramientas se encuentran situadas en Barcelona, hemos adoptado una perspectiva decolonial, antirracista y feminista. Por ello, la metodología empleada incorpora el conocimiento y la experiencia de las organizaciones y defensoras de derechos humanos que hemos entrevistado en varios países del Mashreq y el Maghreb.

Existe una interdependencia tecnológica en la que el norte global extrae las materias primas de los países del sur global, para fabricar tecnologías que se testean sobre las poblaciones de estos países y que después se usan para perfeccionar la vigilancia sobre defensoras de derechos humanos, periodistas, oposición política, disidentes de género y sexuales o personas migrantes en todo el mundo.

Consideramos que este contexto nos obliga a identificar y conocer las implicaciones que la vigilancia masiva tiene en los derechos humanos y en las personas defensoras de toda la región mediterránea, y así asumir la responsabilidad que tenemos desde el norte global.

---

4 **SMEX.** "Digital Rights During the War on Lebanon". 10 de octubre de 2024. Disponible en: https://smex.org/digital-rights-during-the-war-on-lebanon-october-9-2024/.

5 **ODHE.** «Mass Surveillance.» Disponible en: https://mass-surveillance.odhe.cat/.

I

MARRUECOS: EL PANÓPTICO ALAUÍ

La vigilancia digital en Marruecos recae especialmente sobre periodistas independientes, personas defensoras de derechos humanos y sobre la población saharaui (ver capítulo Sáhara Occidental). La represión de personas disidentes con visibilidad es una estrategia muy efectiva, ya que refuerza la sensación de control total sobre el resto de la población que recurre a la autocensura para evitar la represión. Marruecos ejerce además vigilancia sobre personas de interés fuera del país (desde presidentes y jefes de Estado, hasta periodistas extranjeros). La aparente arbitrariedad ha formado siempre parte de la estrategia represiva del régimen. Por un lado, la persecución a grandes figuras asegura que ningún perfil alto está protegido, y por otro la represión a la población anónima propaga la idea del control total: el panóptico alauí[6] .

“La represión de personas disidentes que tienen visibilidad pública refuerza la sensación de control total sobre el resto de la población, que recurre a la autocensura para evitar la represión”

Los atentados de Casablanca de mayo de 2003 aceleraron la entrada de Marruecos en el marco de lucha antiterrorista promovida desde los Estados Unidos[7]. La ley antiterrorista de 2003, polémica, pero aprobada por unanimidad tras los atentados, dio manga ancha para monitorear los medios de comunicación y los contenidos de sitios web, blogs y otros espacios. Miles de personas fueron detenidas y encarceladas sin cargos durante días[8] y se vigiló a organizaciones, movimientos y defensoras de derechos humanos críticas con el régimen bajo la laxa justificación de la ‘seguridad nacional’ y el ‘orden público’[9].

6 La primera detención conocida por contenido personal online fue en febrero de 2008. La detención por parte de agentes de paisano de Fouad Mourtada por haber creado un perfil falso del hermano del rey, destapó la posible vigilancia masiva online. Fouad no era un activista conocido.

7 En realidad, la colaboración con Estados Unidos en su “Guerra contra el Terror” ya había empezado antes del 2003. Marruecos fue uno de los países que aportó *black sites* (nombre con el que se denomina a centros clandestinos de detención operados por la CIA, generalmente ubicados fuera del territorio continental estadounidense y de su jurisdicción) para el secuestro y tortura de prisioneros tras los atentados de 2001. **Tom Finn.** “How Arab states helped the CIA with its torture-linked rendition program.” Middle East Eye, 13 de febrero de 2015.
Disponible en:
https://www.middleeasteye.net/news/how-arab-states-helped-cia-its-torture-linked-rendition-program.

8 La ley antiterrorista de 2003 permite, además, tener detenida a una persona sin pasar a disposición judicial hasta 12 días. **Human Rights Watch**. “Stop Looking for Your Son. Illegal Detentions under the Counterterrorism Law.” 25 de octubre de 2010.
Disponible en:
https://www.hrw.org/report/2010/10/25/morocco-stop-looking-your-son/illegal-detentions-under-counterterrorism-law.

9 Además, los delitos de opinión contra la monarquía, la religión y la ‘soberanía nacional’ pueden acarrear hasta seis años de prisión. **Departamento de Estado, EUA**. “Morocco 2023 Human Rights Report.”
Disponible en:
https://www.state.gov/wp-content/uploads/2024/02/528267_MOROCCO-2023-HUMAN-RIGHTS-REPORT.pdf.

Desde principios de los 2000, Marruecos ha ido adoptando leyes para controlar la esfera digital (Ley de Cibercrimen en 2003, Ley de Ciberseguridad en 2020)[10]. En septiembre de 2011 se creó la Dirección General de Seguridad de los Sistemas de Información[11] y el maCERT, el "centro de vigilancia, detección y respuesta a los ataques informáticos". Tanto la Dirección como el maCERT están bajo la dirección de la Administración de Defensa Nacional[12], que equivale al Ministerio de Defensa. Esto supone que una parte de la infraestructura de control se ha creado no bajo el paraguas del Ministerio de Interior o de Información, sino dentro de una institución militar en la cual la rendición de cuentas y la transparencia están ausentes[13].

Pese a que, según *Freedom House,* Marruecos es 'parcialmente libre'[14] en el acceso y libertades en internet, la adopción de leyes de prensa y de libertades con estándares más o menos aceptables esconde un uso pernicioso del sistema judicial y del código penal[15]. La mayoría de defensoras de derechos humanos y periodistas no han sido acusadas ni condenadas bajo la Ley de Prensa y Publicaciones, sino en el marco de crímenes tipificados en el Código Penal y que comportan penas de prisión. Se conjugan en ello una legislación represiva, la connivencia necesaria del sistema judicial y una red de tecnologías intrusivas, muchas de ellas desarrolladas por empresas europeas.

10 **Ley 07-03** (2003). Disponible en: https://www.dgssi.gov.ma/sites/default/files/legislative/brochure/2023-03/loi%2007-03.pdf.

11 La Dirección General de Seguridad de Sistemas de Información fue creada por Decreto N° 2-11-509 del 21 septiembre 2011. Es una administración adjunta a la Administración de Defensa Nacional.

12 Hassan II abolió el Ministerio de Defensa en 1972. Actualmente la Administración de Defensa Nacional (ADN) depende directamente del rey a través del ministro delegado de la ADN, también ministro de Interior, Abdellatif Loudiyi.

13 **Freedom House**, "Freedom on the Net 2023: Morocco," acceso 12 de septiembre de 2024. Disponible en: https://freedomhouse.org/country/morocco/freedom-net/2023.

14 **Freedom House**, "Freedom on the Net 2023: Morocco." Disponible en: https://freedomhouse.org/country/morocco/freedom-net/2023.

15 **Committee to Protect Journalists**, "End campaign against independent media in Morocco," 9 de noviembre de 2009. Disponible en: https://cpj.org/2009/11/cpj-urges-morocco-end-campaign-against-independent/.

1. LAS REDES SOCIALES, MOVILIZACIÓN Y MIEDO A PERDER EL CONTROL DEL RELATO

El aumento del uso de las redes sociales supuso un problema para el régimen que, con casos como el *sniper* de Targuist[16] [17], desde 2007 veía cómo la población podía denunciar al sistema por sí misma. El mayor punto de inflexión en la vigilancia digital fue, sin embargo, durante las revueltas de 2011 y el Movimiento 20 de febrero[18]. El gran poder de movilización de la sociedad civil en las revueltas de 2011 que se extendió por la región se llevó a cabo a través de internet, en concreto a través de Facebook y Youtube. Es el caso de la campaña *Mamfakinch*, organizada por un colectivo social días antes de las primeras protestas de febrero[19] [20].

De hecho, una de las primeras compras marroquíes para el control digital en conocerse fue la del *malware*[21] de Hacking Team en formato troyano[22] de activación remota a la tecnológica italiana. Fue usado contra periodistas y contra la campaña *Mamfakinch*[23]. Entre los clientes estaban dos agencias de inteligencia marroquíes (Consejo Superior de la Defensa Nacional - CSDN y la Dirección General de Vigilancia Territorial - DST), obtenidas en 2009 y 2012 respectivamente[24].

---

16 **Jeune Afrique**, "Corruption au Maroc : le « sniper de Targuist » poursuit son combat à visage découvert," 4 de marzo de 2013. Disponible en: https://www.jeuneafrique.com/171981/politique/corruption-au-maroc-le-sniper-de-targuist-poursuit-son-combat-visage-d-couvert/.

17 **AlQarratTV**, "Maroc : Le « Sniper de Targuist » révèle son identité." Disponible en: https://www.youtube.com/watch?v=l9lVKf5Hk4Q.

18 Movimiento de masas cuyas demandas políticas incluían la reforma del sistema político del país.

19 **Samia Errazzouki,** "Under watchful eyes: Internet surveillance and citizen media in Morocco, the case of Mamfakinch," The Journal of North African Studies. Disponible en: https://www.academia.edu/34822277/Under_watchful_eyes_Internet_surveillance_and_citizen_media_in_Morocco_the_case_of_Mamfakinch

20 Pese a la represión, varias campañas de movilización en internet tuvieron un gran impacto como la de Septiembre 2018, #Masaktach ("NoCallaré") contra la violencia machista y el acoso sexual; o la campaña de boicot el mismo año contra varias empresas estrechamente ligadas al régimen (Central Danone, Sidi Ali, Afriquia). **Freedom House**. "Freedom on the Net 2019." Disponible en: https://freedomhouse.org/country/morocco/.

21 Ver glosario.

22 Ver glosario.

23 **Privacy International.** "Their Eyes on Me: Stories of Surveillance in Morocco." 7 de abril de 2015. Disponible en: https://privacyinternational.org/report/1125/their-eyes-me-stories-surveillance-morocco.

24 Ibid.

En octubre de 2016, irrumpieron las masivas protestas de Hirak Rif (Movimiento Popular del Rif), que congregó durante semanas a miles de personas en Al Hoceima y otras poblaciones del norte de Marruecos. Además de la represión in situ, entre mayo y agosto de 2017 defensoras de derechos humanos, periodistas o blogueras fueron detenidas por sus actividades en internet[25] [26].

2. LA MANIPULACIÓN DE LAS REDES SOCIALES

Actualmente, las redes sociales son la fuente principal de información de la población marroquí, con Youtube y Facebook en cabeza[27], ya que son las únicas formas de comunicación que se salen del discurso oficial. Por tanto, son estas redes en las que se centra el control y la represión, que se lleva a cabo con distintos tipos de estrategias.

Una de ellas ha sido la utilización de redes de comportamiento inauténtico coordinado[28] que buscaban influir en la opinión pública tanto a nivel local como regional. Meta eliminó cientos de cuentas en Facebook e Instagram vinculadas a actividades progubernamentales, que elogiaban la gestión del Gobierno marroquí frente a la pandemia, sus iniciativas diplomáticas y la respuesta de las fuerzas de seguridad, además de alabar al rey Mohammed VI y a altos funcionarios de seguridad[29] [30]. Las cuentas estaban relacionadas con medios prorégimen como ChoufTV, conocida por su trabajo difamatorio contra defensoras de derechos humanos[31]. Según Meta, unas 150.000 cuentas seguían a una o más de estas páginas.

---

25 Activistas pacíficos como Nasser Zefzafi y El Mortada Iamrachen fueron acusados de 'romper el respeto al rey', 'ofender las instituciones constitucionales' o 'insultar a cargos públicos'. Rabieh Al-Ablaq fue sentenciado en junio de 2017 a 5 años de prisión por "publicación de noticias falsas" y "usurpación del título de periodista". Al-Ablaq denunció las torturas sufridas durante los interrogatorios de la policía en Al Hoceima.

26 **Access Now**, "Morocco: A complete blackout during protests in Al-Hoceima," 30 de noviembre de 2017. Disponible en: https://www.accessnow.org/morocco-complete-blackout-protests-al-hoceima/.

27 Hay, sin embargo, diferencias sustanciales entre el acceso y uso de internet por parte de hombres y mujeres, entre la población rural y urbana, y entre jóvenes o gente mayor de 30. **Arab Barometer.** "The MENA Digital Divide," septiembre de 2020.
Disponible en: https://www.arabbarometer.org/2020/09/the-mena-digital-divide/.

28 Ver glosario.

29 **Meta.** "December 2020 Coordinated Inauthentic Behavior Report," 12 de enero de 2021.
Disponible en:
https://about.fb.com/news/2021/01/december-2020-coordinated-inauthentic-behavior-report/.

30 Sólo en febrero de 2021, se eliminaron en Marruecos 385 cuentas y 6 páginas de Facebook, así como 40 cuentas de Instagram operadas desde Marruecos y dirigidas al público general. Esta red de cuentas fue desmantelada por Meta después de las denuncias de Amnistía Internacional. Facebook, "February 2021 CIB Report,". Marzo de 2021.
Disponible en: https://about.fb.com/wp-content/uploads/2021/03/February-2021-CIB-Report.pdf.

31 **ADN (por sus siglas en francés)**, "Defamation Campaign against Human Rights Defender Karima Nadir," Frontline Defenders.
Disponible en: https://www.frontlinedefenders.org/en/case/defamation-campaign-against-woman-human-rights-defender-karima-nadir.

3. VIGILANCIA Y CONTROL MASIVO DE LAS COMUNICACIONES

La vigilancia y control masivo de las comunicaciones se hace con el apoyo de tecnologías punta. Ello conlleva un control de la información que circula y se publica, pero también apagones digitales puntuales[32]. Aunque el filtrado (bloqueo de determinados sitios e informaciones) no es una de las herramientas más utilizadas, se sigue usando de manera arbitraria y sin aviso oficial[33]. Destacan los mecanismos de vigilancia especialmente intrusivos hacia defensoras de derechos humanos y personas críticas con el régimen.

En 2019, Amnistía Internacional denunció que los dispositivos de destacadas defensoras de los derechos humanos habían sido infectados por Pegasus. Entre ellos, la defensora saharaui Aminatou Haidar, el historiador Maati Monjib, los periodistas e investigadores Taoufik Bouachrine, Omar Radi, Soulaimane Raissouni; o el abogado de derechos humanos Abdessadak El Bouchattaoui. Según los periodistas, algunos de los contenidos y materiales obtenidos a través de Pegasus fueron usados para difamarlos, chantajearlos y acosarlos.

En 2022, Amnistía Internacional y Citizen Lab encontraron pruebas sólidas del uso de este *spyware*[34] Pegasus, de la israelí NSO Group, por parte de las autoridades marroquíes y se hizo una lista de posibles afectadas con hasta 10.000 personas, incluyendo al propio rey Mohammed VI[35] [36]. Marruecos también espió a defensoras de derechos humanos saharauis, y a figuras prominentes en el extranjero, como periodistas franceses y el presidente Emmanuel Macron; españoles como el presidente del Gobierno, Pedro Sánchez, la ministra de Defensa, y los de Interior y Agricultura. Aunque NSO no ha negado el uso de su software en estos casos, tampoco ha publicado los resultados de una investigación que

32 Del 25 al 30 de mayo de 2007, YouTube fue bloqueado por la mayor empresa de telecomunicaciones, Maroc Telecom (las otras dos proveedoras Wana y Meditel no lo bloquearon). **Global Voices**, "Morocco Blocks Access to Youtube,". 26 de mayo de 2007.
Disponible en: https://globalvoices.org/2007/05/26/morocco-blocks-access-to-youtube/.

33 En enero de 2016, Maroc Telecom, Meditel and Inwi bloquearon llamadas a través de Internet (VoIP) en 3G y 4G (Skype, Viber, Tango, WhatsApp and Facebook Messenger entre otras). **Saad Guerraoui**, "Morocco banned Skype, Viber, WhatsApp and Facebook Messenger. It didn't go down well," **Middle East Eye**. 9 de marzo de 2016.
Disponible en:
https://www.middleeasteye.net/opinion/morocco-banned-skype-viber-whatsapp-and-facebook-messenger-it-didnt-go-down-well.

34 Ver glosario.

35 **Forbidden Stories.** "About the Pegasus Project." Forbidden Stories. 18 de julio de 2021.
Disponible en: https://forbiddenstories.org/about-the-pegasus-project/.

36 **El País.** "Macron, en el punto de mira del programa de espionaje Pegasus contratado por Marruecos." El País. 20 de julio de 2021.
https://elpais.com/internacional/2021-07-20/macron-en-el-punto-de-mira-del-programa-de-espionaje-pegasus-contratado-por-marruecos.html.

prometió realizar en 2019. Además, el Ministerio de Interior marroquí habría sido cliente[37] de Circles Technologies al menos desde 2018, utilizando un sistema de esta empresa, afiliada a NSO Group, para controlar llamadas, mensajes de texto y ubicaciones a partir de vulnerabilidades de las redes.

Por otro lado, el grupo de periodismo de investigación francés Reflet destapó la compra de Eagle System por parte de Marruecos[38]. Un sistema de vigilancia digital masiva de tráfico de Internet con funciones de censura (a través de Deep Packet Inspection[39]), propiedad de la empresa francesa Amesys (Nexa Technologies). En 2011, Marruecos había invertido alrededor de 2 millones de euros en el sistema Eagle, desarrollado bajo el nombre de "Project Popcorn"[40].

La investigación de la organización Citizen Lab también destapó la compra del *malware*[41] FINFIsher[42] por parte del Consejo Superior de la Defensa Nacional de Marruecos[43]. FINFIsher (o Finspy), de la empresa angloamericana Gamma Group, se vende exclusivamente a agencias gubernamentales y fuerzas policiales a través de Lench IT Solutions plc. El software controla de forma remota cualquier aparato previamente infectado y puede copiar archivos, interceptar llamadas de Skype y registrar incluso los movimientos del teclado.

37 **Citizen Lab**. "Running in Circles: Uncovering the Clients of Cyberespionage Firm Circles." Citizen Lab, 2020. https://citizenlab.ca/2020/12/running-in-circles-uncovering-the-clients-of-cyberespionage-firm-circles/.

38 **Privacy International**. "Their Eyes On Me: Stories of Surveillance in Morocco". 2015. Disponible en: https://privacyinternational.org/report/1125/their-eyes-me-stories-surveillance-morocco.

39 Ver glosario.

40 **Reflets.info**, "Maroc : Popcorn, le projet qui n'existait pas," 15 de noviembre de 2017. Disponible en: https://reflets.info/articles/maroc-popcorn-le-projet-qui-n-existait-pas.

41 **Ver glosario.**

42 **Bill Marczak, John Scott-Railton, Adam Senft, Irene Poetranto, y Sarah McKune**. "Pay No Attention to the Server Behind the Proxy Mapping FinFisher's Continuing Proliferation," Citizen Lab, 15 de octubre de 2015. Disponible en: https://citizenlab.ca/2015/10/mapping-finfishers-continuing-proliferation/.

43 **Charlie Osborne**, "In Hacking Team's wake, FinFisher spyware rises in popularity with government users," *ZDNet*, 19 de octubre de 2015. Disponible en: https://www.zdnet.com/article/in-hacking-teams-wake-finfisher-spyware-rises-in-popularity-with-government-users/.

4. ACOSO ONLINE: CAMPAÑAS DE DESPRESTIGIO Y EMBOSCADAS DIGITALES[44]

En los ataques y trolling online[45] han destacado las campañas de desprestigio, estrategia muy utilizada en Marruecos. Human Rights Watch lo denomina *character assassination campaigns* (campañas de asesinato al personaje), en las que, de manera aparentemente orquestada, se inician campañas de difamación y bulos[46]. Muy a menudo estas campañas atacan las libertades sexuales de las defensoras de derechos humanos. En un informe de Meta de diciembre de 2021[47], se menciona a Marruecos como origen de perfiles de cuentas de Facebook e Instagram vinculadas al software israelí Cognyte (antigua WebintPro). Este software permite la creación y gestión de cuentas falsas en redes sociales como Facebook, Instagram, Twitter y YouTube. También recoge datos de estas redes sociales. Según el mismo informe de Meta su objetivo apunta principalmente a periodistas y políticas[48]. Además, se han identificado grupos de hackers que actúan para sabotear contenido crítico en las redes o infiltrarse en redes sociales o correos electrónicos privados[49].

"Las mujeres defensoras periodistas o personalidades públicas críticas con el gobierno son especialmente atacadas con violencia machista online, con continuas campañas de difamación sobre su libertad sexual y acoso"

Las mujeres defensoras periodistas o personalidades públicas críticas con el Gobierno son especial-

44 Ver glosario.

45 Ver glosario.

46 **Human Rights Watch**, "'They'll Get You No Matter What': Morocco's Playbook to Crush Dissent," 28 de julio de 2022. Disponible en: https://www.hrw.org/report/2022/07/28/theyll-get-you-no-matter-what/moroccos-playbook-crush-dissent.

47 **Mike Dvilyanski, David Agranovich y Nathaniel Gleicher**, "Threat Report on the Surveillance-for-Hire Industry," Meta, 16 de diciembre de 2021. Disponible en: https://about.fb.com/wp-content/uploads/2021/12/Threat-Report-on-the-Surveillance-for-Hire-Industry.pdf.

48 **Mike Dvilyanski, David Agranovich y Nathaniel Gleicher**, "Threat Report on the Surveillance-for-Hire Industry," Meta, 16 de diciembre de 2021. Disponible en: https://about.fb.com/wp-content/uploads/2021/12/Threat-Report-on-the-Surveillance-for-Hire-Industry.pdf.

49 En septiembre de 2013, la web de Investigative Journalism en Marruecos fue hackeada y sus contenidos sustituidos por porno (una estrategia habitual). La plataforma independiente de información, Lakome.com fue bloqueada judicialmente el 17 de octubre de 2013 y no ha conseguido restablecerse. Su director y periodista, Ali Anouzla, fue también detenido bajo la Ley Antiterrorista por haber enlazado un artículo sobre AlQaeda. **Reporters Without Borders**, "Website editor held for posting Al Qaeda video," 20 de septiembre de 2013. Disponible en: https://web.archive.org/web/20150610182747/http://en.rsf.org/morocco-website-editor-held-for-posting-19-09-2013,45197.html.

mente atacadas con violencia machista online, con continuas campañas de difamación sobre su libertad sexual y acoso[50]. ChoufTV, publicó en 2020 información difamatoria de la activista por los derechos de las mujeres Karima Nadir[51].

Human Rights Watch denuncia también los ataques de entrampamiento digital[52] contra personas de la comunidad LGBTIQ+. En 2020, se orquestó una campaña homófoba de outing[53] forzado de hombres gays o bisexuales a través de apps[54]. Las relaciones sexuales entre personas del mismo sexo están prohibidas en Marruecos y además de la persecución judicial, estas informaciones pueden traer consecuencias sociales graves para las personas, como violencia física directa, represalias profesionales, etc.

La represión sufrida online deriva a menudo en tres consecuencias: autocensura, sexilio[55] o represión física. Siguiendo las campañas de difamación sexualizadas, el periodista Taoufik Bouachrine, director del diario Akhbar al Yaum, fue condenado en 2018 a 15 años de cárcel por varios delitos (trata de personas, agresión sexual, violación, prostitución y acoso) tras una agitada campaña mediática[56]. Su colega Hajar Raissouni fue arrestada en 2019 bajo los cargos de "aborto ilegal" y "relaciones sexuales fuera del matrimonio" y por estar embarazada de su jefe[57]. Las autoridades marroquíes intentaron probar los cargos a toda costa, incluso obligándola a someterse a un examen médico sin su consentimiento. Fue condenada a un año de prisión, antes de ser liberada gracias a un indulto real[58] y forzada a irse del país.

---

50 **Freedom House**, "Freedom on the Net 2023: Morocco."
Disponible en: https://freedomhouse.org/country/morocco/freedom-net/2023.

51 Llamando a su detención, acusándola de consumo de drogas y madre soltera negligente. Karima Nadir es cofundadora del 490 Collective y vicepresidenta de la Asociación por los Derechos Digitales.

52 Ver glosario.

53 Ver glosario.

54 **Human Rights Watch**, "Morocco: Online Attacks Over Same-Sex Relations," 27 de abril de 2020.
Disponible en: https://www.hrw.org/news/2020/04/27/morocco-online-attacks-over-same-sex-relations.

55 Se refiere a la situación en la que personas del colectivo LGBTIQ+ se ven obligadas a abandonar su lugar de origen debido a la discriminación, el rechazo o la violencia que enfrentan por su orientación sexual o identidad de género.

56 La organización Euro-Mediterranean Human Rights Monitor identificó más de 30 páginas y periódicos online pro-régimen que habían participado en campañas de esta índole. **Reporters Without Borders**, "After long jail term, Moroccan journalist hit by heavy damages award," 7 de diciembre de 2018.
Disponible en: https://rsf.org/en/after-long-jail-term-moroccan-journalist-hit-heavy-damages-award.

57 **Human Rights Watch**, "Morocco: Trial Over Private Life Allegations," 9 de septiembre de 2019.
Disponible en: https://www.hrw.org/news/2019/09/09/morocco-trial-over-private-life-allegations.

58 El perdón real se repite en ocasión de fiestas nacionales importantes. En esas ocasiones se publica una lista de 'perdones' que el rey otorga a personas previamente condenadas por la justicia. La arbitrariedad del Perdón Real es obvia. En 2020, el perdón real incluyó a miembros del Movimiento Popular del Rif. En 2024 fueron 'perdonados' varios periodistas de alto perfil: Omar Radi, Souleimane Raissouni y Taoufik Bouachrine, Hicham Mansouri, Samad Ait Aicha, Imad Stitou, y Afaf Bernani.

II

EL SÁHARA OCCIDENTAL: VIGILANCIA PARA MANTENER LA OCUPACIÓN

Desde la ruptura de la tregua de 1991 entre el Frente Polisario y Marruecos, y tras la incursión de las fuerzas marroquíes el 13 de noviembre de 2020 para expulsar a un grupo de activistas saharauis que protestaban por el expolio de recursos del Sáhara Occidental ocupado por Marruecos, las hostilidades entre ambos actores se han intensificado. Paralelamente, también ha aumentado la represión y la persecución de las organizaciones y defensoras pro-saharauis.

1. LA MODERNIZACIÓN DE LOS SISTEMAS DE VIGILANCIA DE MARRUECOS

La ocupación de Marruecos del territorio del Sáhara Occidental ha dependido, en gran parte, de la capacidad de controlar, vigilar, y reprimir a la población autóctona saharaui. Desde el año 2020, la situación de los derechos humanos en el territorio ocupado del Sáhara Occidental se ha vuelto más alarmante. La creciente digitalización en el panorama africano y marroquí ha influido en los métodos, el impacto y el aumento de las estrategias de vigilancia sobre la población del Sáhara Occidental[59]. Además, el acercamiento de Marruecos a Israel, desde el restablecimiento de relaciones en 2020[60], ha permitido su colaboración en la modernización y el desarrollo de instrumentos de inteligencia y vigilancia. Paralelamente desde 2009 se identifican acuerdos con la empresa española Indra Sistemas, S.A. Indra firmó un contrato por 6,3 millones de euros para instalar tres estaciones que ampliaban su red de vigilancia por satélite en las ciudades de El Aaiún, Smara y Dajla[61]. En mayo de 2024 Indra y la Agencia de Desarrollo Digital (ADD) de Marruecos han firmado un acuerdo destinado a acelerar el proceso de transformación digital en Marruecos[62].

La vigilancia de población civil saharaui por parte de las autoridades marroquíes se ha basado en el uso de su mano de obra, la introducción de informantes y colonos, el control de las fronteras, el aislamiento de la población y la persecución y represión de la disiden-

59 **Lara Jakes, Isabel Kershner, Aida Alami, and David Halbfinger.** "Morocco Joins List of Arab Nations to Begin Normalizing Relations With Israel," The New York Times. 10 de diciembre de 2020. Disponible en: https://www.nytimes.com/2020/12/10/world/middleeast/israel-morocco-trump.html.

60 **Lara Jakes, Isabel Kershner, Aida Alami, and David Halbfinger.** "Morocco Joins List of Arab Nations to Begin Normalizing Relations With Israel," The New York Times. 10 de diciembre de 2020. Disponible en: https://www.nytimes.com/2020/12/10/world/middleeast/israel-morocco-trump.html.

61 Indra. "Marruecos mejorará la gestión de tráfico aéreo con tecnología de Indra." 29 de octubre de 2009. https://www.indracompany.com/es/noticia/marruecos-mejorara-gestion-trafico-aereo-tecnologia-indra.

62 **El Economista.** "Indra impulsará la transformación digital de Marruecos." El Economista. 17 de mayo de 2024. https://www.eleconomista.es/telecomunicaciones/noticias/12841197/05/24/indra-impulsara-la-transformacion-digital-de-marruecos.html.

cia[63]. Las autoridades marroquíes han estado sometiendo a la población saharaui a una vigilancia constante, tanto física como tecnológica[64]; como informan medios como Por Un Sáhara Libre (PUSL)[65]. Otras fuentes denuncian la instalación de cámaras de vigilancia en El Aaiún, Smara, Dajla e incluso en ciudades más pequeñas del Sáhara Occidental ocupado por Marruecos[66].

Los dos órganos principales que llevan a cabo esta vigilancia son las fuerzas policiales marroquíes y la Dirección General de Vigilancia Territorial (DGTS por sus siglas en francés), el órgano gubernamental del servicio de inteligencia civil de Marruecos. Estos dos órganos de las fuerzas marroquíes[67] están integrando nuevas tecnologías en sus estrategias y mecanismos de control. Desde 2023, el DGTS colabora con el *Federal Bureau of Investigation* (FBI) estadounidense en una alianza "antiterrorista" que aborda la zona "sahara-saheliana"[68] y que acaba facilitando el control sobre las disidencias en el territorio.

63 **ECSaharaui**. "Marruecos intensifica su espionaje en el Sáhara Occidental ocupado por temor a un levantamiento popular." 7 de agosto de 2024.
https://ecsaharaui.com/07/2024/marruecos-intensifica-su-espionaje-en-el-sahara-occidental-ocupado-por-temor-a-un-levantamiento-popular/.

64 **Amnesty International**, "Derechos Pisoteados: Protestas, Violencia y Represión en el Sáhara Occidental," 2010. Disponible en: https://www.amnesty.org/es/wp-content/uploads/sites/4/2021/07/mde290192010es.pdf.

65 **Por un Sáhara Libre**. "Página oficial sobre la situación del Sáhara Occidental y la lucha por la autodeterminación." Recuperado de https://porunsaharalibre.org/.

66 **ECSaharaui**. "Sáhara Occidental: Marruecos espía con cámaras de reconocimiento a los saharauis en El Aaiún ocupado." 7 de agosto de 2024.
https://ecsaharaui.com/07/2024/sahara-occidental-marruecos-espia-con-camaras-de-reconocimiento-a-los-saharauis-en-el-aaiun-ocupado/.

67 **Amnesty International**, "Derechos Pisoteados: Protestas, Violencia y Represión en el Sáhara Occidental," 2010. Disponible en:
https://www.amnesty.org/es/wp-content/uploads/sites/4/2021/07/mde290192010es.pdf.

68 **Swissinfo**, "El FBI y la DGST marroquí amplían su colaboración antiterrorista en el Sahel," 21 de febrero de 2023. Disponible en:
https://www.swissinfo.ch/spa/el-fbi-y-la-dgst-marroqu%C3%AD-ampl%C3%ADan-su-colaboraci%C3%B3n-antiterrorista-en-el-sahel/48304956.

2. COVID-19: DE LA VIGILANCIA INSTITUCIONAL A LA 'AUTOVIGILANCIA'

El Estado marroquí declaró el estado de emergencia el 20 de marzo de 2020 con el objetivo de proteger a la población de la pandemia de COVID-19[69]. El 23 de marzo de 2020 se aprobó el estado de emergencia con la Ley No. 2.20.292, que establece penas y multas para cualquiera que incumpla "órdenes y decisiones de las autoridades" y para cualquiera que "obstruya" dichas decisiones, incluyendo la difusión de "escritos, publicaciones o fotos" en redes sociales[70].

En términos de tecnología, una de las principales iniciativas fue el desarrollo de una aplicación móvil por ingenieros y técnicos de la Dirección General de la Seguridad Nacional marroquí (DGSN) con el apoyo del Ministerio de Sanidad y el Ministerio del Interior[71]. La aplicación Wiqaytna, es una herramienta voluntaria para identificar a personas que hayan estado en contacto con alguien positivo por COVID-19. La *app* cumple con la Ley No. 09-08, cuyo artículo 4 no obliga a las autoridades a obtener el consentimiento de una persona para procesar sus datos personales cuando se emplean para la amplia tarea de proteger el interés público. Esto permite un control masivo de los movimientos de la población[72].

Las autoridades marroquíes terminaron oficialmente el estado de emergencia sanitaria en febrero 2023[73] hecho que desactivó la Ley No. 2.20.292, pero se puede observar como la estrategia de autovigilancia y censura poblacional se ha traducido en otras políticas de cibervigilancia. En junio de 2024, la Dirección General de Seguridad Nacional lanzó la plataforma E-Blagh[74] que permite a la sociedad civil denunciar cibercrímenes y notificar directamente a las autoridades de alguna infracción o crimen digital, hecho que según el

69 **Europa Press Internacional**, "Marruecos declara el estado de emergencia desde este viernes y 'hasta nuevo aviso' por el coronavirus," 20 de marzo de 2020.
Disponible en:
https://www.europapress.es/internacional/noticia-marruecos-declara-estado-emergencia-viernes-nuevo-aviso-coronavirus-20200320025538.html.

70 **Projet de loi n° 22.20**, "relatif à l'usage des réseaux sociaux et des plateformes de communication au Maroc," presentado al Parlamento del Reino del Marruecos, 2020.
Disponible en: https://www.cg.gov.ma/fr/node/9696.

71 **Access Now**, "COVID-19 Contact-Tracing Apps in MENA: A Privacy Nightmare". 18 de junio de 2020.
Disponible en: https://www.accessnow.org/COVID-19-contact-tracing-apps-in-mena-a-privacy-nightmare/.

72 **Access Now**, "COVID-19 Contact-Tracing Apps in MENA: A Privacy Nightmare."
Disponible en: https://www.accessnow.org/COVID-19-contact-tracing-apps-in-mena-a-privacy-nightmare

73 **Crisis 24**, "Morocco: Officials End Health State of Emergency as of Feb. 28 / Update 106," 28 de febrero de 2024.
Disponible en:
https://crisis24.garda.com/alerts/2023/02/morocco-officials-end-health-state-of-emergency-as-of-feb-28-update-106?origin=fr_riskalert.

74 **H24Info**, "La Plateforme de Lutte Contre la Cybercriminalité Désormais Opérationnelle," 4 de junio de 2024.
Disponible en:
https://www.h24info.ma/e-blagh-la-plateforme-de-lutte-contre-la-cybercriminalite-desormais-operationnelle/.

artículo 267-591 del Código Penal marroquí incluye "cualquier amenaza a la integridad del reino de Marruecos". El desarrollo de esta plataforma involucra a la población para reportar y controlar el cibercrimen[75].

3. EL CONTROL DE LOS MEDIOS DE COMUNICACIÓN Y LA PERSECUCIÓN DE PERIODISTAS

El control de los medios de comunicación y la censura del periodismo han sido estrategias claves del Gobierno marroquí para mantener el control sobre el Sáhara Occidental y defender su legitimidad a nivel internacional[76]. Según un informe de Reporteros Sin Fronteras sobre las violaciones contra el sector periodístico en este conflicto, "el periodismo es una de las muchas víctimas de este conflicto olvidado por los medios, que ha convertido al Sáhara Occidental en un verdadero 'agujero informativo'"[77]. El desarrollo digital ha afectado a las periodistas saharauis, a través de la persecución mediante medios digitales. En palabras del periodista Ahmed Ettanji de Equipe Media, "la represión digital es una cuestión también muy importante, porque la mayoría de nuestro trabajo es digital, se basa en las redes sociales y más en los medios de comunicación alternativos"[78]. Según Ettanji, esto tiene un "impacto individual, en la limitación del movimiento, porque se está vigilado. Ya sea física o tecnológicamente, impidiendo trabajar de una forma libre"[79].

Además, las mujeres periodistas sufren de una doble vulnerabilidad, como fue en el caso de Nazha el Khalidi, quien fue interrogada y torturada por las fuerzas policiales marroquíes y además sufrió difamación de carácter machista[80]. En esta línea, según

75 **MAP Express**. "La DGSN lanza la nueva plataforma 'E-Blagh' dedicada a la lucha contra la ciberdelincuencia." 6 de junio de 2024. https://www.mapexpress.ma/actualite/societe-et-regions/dgsn-lance-nouvelle-plateforme-e-blagh-dediee-lutte-contre-cybercriminalite/.

76 **Amnesty International**, "Marruecos y el Sáhara Occidental 2023." Disponible en: https://www.amnesty.org/es/location/middle-east-and-north-africa/north-africa/morocco-and-western-sahara/report-morocco-and-western-sahara/.

77 **Reporteros Sin Fronteras**, "Marruecos/Sáhara Occidental," Reporteros Sin Fronteras. Disponible en: https://rsf.org/es/pais/marruecos-sahara-occidental.

78 Ahmed Ettanji, entrevista realizada en el marco de The Nonviolence Factory, noviembre de 2023. Equipo NOVACT, SUDS, IRIDIA y ODHE.

79 Ibid

80 **Reporteros Sin Fronteras**, "Sáhara Occidental, un desierto para el periodismo," 2019. Disponible en: https://www.rsf-es.org/wp-content/uploads/attachments/2019_SAHARA_OCCIDENTAL_RSF_ES_INFORME.pdf.

el informe de OpenNet Initiative de 2007[81], Marruecos ha censurado numerosos sitios web, principalmente aquellos que apoyan la independencia del Sáhara Occidental, como la página de la Unión de Periodistas y Escritores Saharauis[82].

El Gobierno de Marruecos emplea principalmente el *spyware*[83] espía Pegasus, perteneciente al grupo israelí NSO Group, como herramienta de persecución y control a periodistas. Según Amnistía Internacional, esta tecnología también se ha utilizado para espiar a defensoras de derechos humanos saharauis[84], entre ellas a la defensora de derechos humanos Aminatou Haidar[85]. Esta organización acredita que la falta de transparencia en la industria de la vigilancia (por parte de empresas y Gobiernos) dificulta conocer qué herramientas se están utilizando, vendiendo y comprando, lo que impide que las víctimas exijan responsabilidades.

"la falta de transparencia en la industria de la vigilancia dificulta conocer qué herramientas se están utilizando y comercializando, lo que impide que las víctimas exijan responsabilidades"

Los *spywares*[86] son usados frecuentemente para identificar a periodistas disidentes con el objetivo de silenciar su trabajo. Además, el aumento de la persecución contra periodistas saharauis ha hecho más difícil documentar las violaciones de derechos humanos en el Sáhara Occidental desde fuera del territorio. Un caso paradigmático de acoso fue la represión de la pareja de defensoras de derechos humanos saharauis de Equipe Media, Ahmed Ettanji y Naziha El Khalidi, que fueron sometidas a arresto domiciliario e incluso vieron su boda impedida. Se cree que los ataques a periodistas saharauis son una respuesta directa a sus reportajes sobre la represión actual en el territorio ocupado, una actividad que pone

81 **OpenNet Initiative**, "Internet Filtering in Morocco in 2006-2007".
Disponible en: https://opennet.net/studies/morocco2007.

82 **Unión de Periodistas y Escritores Saharauis (UPES)**, "UPES". Disponible en: www.upes.org

83 Ver glosario.

84 **Amnesty International**, "Morocco/Western Sahara: Activist Targeted with Pegasus Spyware in Recent Months – New Evidence," 22 de octubre de 2023.
Disponible en:
https://www.amnesty.org/en/latest/news/2022/03/morocco-western-sahara-activist-nso-pegasus/.

85 **Oscar Rickett**, "Pegasus spyware: Western Sahara activist Aminatou Haidar targeted." Middle East Eye. 9 de marzo de 2022.
Disponible en:
https://www.middleeasteye.net/news/pegasus-spyware-morocco-western-sahara-activist-targeted

86 Ver glosario.

en riesgo su integridad física[87]. La persecución de periodistas saharauis limita su libertad de movimiento, además impidiéndoles realizar su trabajo de manera libre. La persecución también afecta el entorno familiar y la salud mental de las periodistas, generando un impacto económico y deteriorando la cohesión social. En adición, el factor de género ha agravado la vulnerabilidad de las mujeres periodistas, exponiéndolas a mayores riesgos y represalias, como se ha documentado en los casos de violencia, por ejemplo, sufridos por las defensoras saharauis Mbarka Mohamed al-Hafiz y Fatima Mohamed al-Hafiz[88].

4. EL USO DE DRONES: CONTROLAR Y ATACAR DESDE EL AIRE

Tras la disolución del alto al fuego en 2020, que agravó las hostilidades en el territorio, Marruecos ha utilizado la tecnología de drones para establecer su control sobre el territorio. Se han utilizado tanto para realizar ataques como para vigilar las actividades en el territorio ocupado y los campamentos de personas refugiadas[89]. Los ataques de drones están supuestamente dirigidos a combatientes del Frente Polisario, pero su uso ha afectado a civiles de diversas procedencias, agravando la escalada del conflicto más allá del territorio del Sáhara Occidental[90]. Por ejemplo, un ataque con drones marroquíes en 2021 en el Sáhara Occidental, controlado por el Frente Polisario, mató a tres camioneros argelinos[91]. Según *Africa Intelligence*[92], desde 2020 el Gobierno marroquí ha integrado la tecnología de drones para controlar los campamentos saharauis y sus fronteras con Argelia. Desde la escalada del conflicto, en 2021, el Gobierno marroquí celebró un

87 **NOMADS**, "Morocco/Western Sahara: First They Came for the Journalists. We Don't Know What Happened After That," 4 de diciembre de 2020. Disponible en: https://vest-sahara.s3.amazonaws.com/skvs/feature-images/File/249/5fca397eace21_JournalistAppeal_04.12.2020.pdf

88 **Middle East Eye**, "Western Sahara Female Activists Face Rape, Divorce, and House Arrest," 21 de abril de 2022. Disponible en: https://www.middleeasteye.net/news/western-sahara-female-activists-morocco-rape-divorce-house-arrest.

89 **The New Humanitarian**, "Morocco/Sahrawi: Drone Attacks and the Evolving Conflict," 17 de mayo de 2023. Disponible en: https://www.thenewhumanitarian.org/news-feature/2023/05/17/morocco-sahrawi-drone-attacks.

90 **Le Monde**, "Morocco to Become Rare Military Drone Manufacturer Thanks to Cooperation with Israel," 9 de mayo de 2024. Disponible en: https://www.lemonde.fr/en/le-monde-africa/article/2024/05/09/morocco-to-become-rare-military-drone-manufacturer-thanks-to-cooperation-with-israel_6670920_124.html#:~:text=Israeli%20company%20BlueBird%20Aero%20Systems,a%20production%20facility%20in%20Rabat.&text=Joining%20South%20Africa%2C%20Egypt%20and,countries%20that%20build%20military%20drones.

91 **Menadefense**, "Comprendre l'attaque marocaine contre les civils algériens". Disponible en: https://www.menadefense.net/comprendre-lattaque-marocaine-contre-les-civils-algeriens/.

92 **Africa Intelligence**. "Rabat Opts for Yet More Turkish Armed Drones to Contend with Polisario and Algiers," Africa Intelligence, 2 de diciembre de 2021. Disponible en: https://www.africaintelligence.com/north-africa/2021/12/02/rabat-opts-for-yet-more-turkish-armed-drones-to-contend-with-polisario-and-algiers,109708627-art.

contrato con la empresa turca Baykar para la adquisición de los drones Bayraktar TB2[93] especializados en la vigilancia y el reconocimiento[94]. Algunas webs mencionan que desde 2023 Marruecos ha adquirido drones armados Akinci[95], a los que se ha registrado sobrevolando en territorio de Smara, en el Sáhara Occidental ocupado[96]. El informe anual de la organización *Sahrawi Mine Action Coordination Office* (SMACO), destaca 73 ataques con drones marroquíes contra civiles entre 2021 y 2023, resultando en 160 víctimas civiles, incluidas 80 muertes[97]. La naturaleza indiscriminada de estos ataques ha causado graves heridas y muertes entre la sociedad civil saharaui, mauritana y argelina, toda población civil[98]. El desarrollo de la tecnología de drones y el fin del alto al fuego han sido acompañados por el desarrollo de la Ley estructural marroquí No. 10.20[99], que a través de sus 55 artículos permite y fomenta la construcción de unidades para la industria armamentística en Marruecos, la fabricación de armas a través de operadores nacionales, así como fomenta las inversiones extranjeras en este sector[100]. A la par, la normalización de las relaciones entre Marruecos e Israel en 2020[101] ha fomentado la cooperación militar entre estos dos actores, lo que derivó en un memorando de entendimiento en 2021

93 **Institut français des relations internationales** (IFRI), "TB2 Bayraktar: La Grande Stratégie d'un Petit Drone,". 17 de abril de 2023.
Disponible en: https://www.ifri.org/fr/publications/briefings-de-lifri/tb2-bayraktar-grande-strategie-dun-petit-drone.

94 **Baykar**, "Bayraktar TB2,". Disponible en: https://baykartech.com/en/uav/bayraktar-tb2/

95 **Bladi**, "Akinci Zoom: Le Drone que le Maroc Va Acquérir," Bladi.
Disponible en: https://www.bladi.net/akinci-zoom-drone-que-maroc-acquerir,103967.html.

96 **Morocco Mail**. "Le drone Bayraktar TB-2 opérationnel au Sahara Occidental: Maroc-Algerie."
Disponible en:
https://www.moroccomail.fr/2021/11/08/le-drone-bayraktar-tb-2-operationnel-au-sahara-occidental-maroc-algerie/#google_vignette.

97 **SMACO**. "Drone Strikes: SMACO Annual Report 2024" SMACO. 31 de mayo de 2024.
https://sandblast-arts.org/wp-content/uploads/2024/07/SMACO-2024-Report.pdf.

98 Ibid.

99 **Rachid El Houdaigui y Abdelhamid Bakkali**. "Le Régime Juridique de l'Industrie de Défense au Maroc" Policy Paper, Policy Center for the New South, 2023.
Disponible en:
https://www.policycenter.ma/sites/default/files/2022-01/PP-28-21-El%20Houdaigui-BAKKALI-VF.pdf.

100 **Yahia Hatim**. "New Framework Law Sets Ground for Arms Industry in Morocco: The New Legal Text Could Allow Morocco to Stop Relying Solely on Imports in Terms of Weapons and Ammunition," *Morocco World News*. 16 de julio de 2020.
Disponible en:
https://www.moroccoworldnews.com/2020/07/310459/new-framework-law-sets-ground-for-arms-industry-in-morocco.

101 **Juan José Vagni y Ignacio Rivas.** "Marruecos y la Normalización de Relaciones con Israel: Fundamentos y Proyección de una Aproximación Singular," en ¿Y Ahora Adónde Vamos?: Nuevos Desafíos en el Medio Oriente, ed. Juan José Vagni y Ignacio Rivas. 2023.
Disponible en: https://sedici.unlp.edu.ar/handle/10915/162819.

entre los dos países en el ámbito de la defensa[102]. Tras este acuerdo, se han conocido los planes de la empresa israelí Blue Bird Aero Systems para establecer una planta de producción de drones en Marruecos, de los modelos WanderB y ThunderB, destinados principalmente a misiones de reconocimiento, inteligencia y detección de objetivos[103]. El ataque mediante drones está promoviendo el desplazamiento de la población saharaui fuera de su territorio, vulnerando sus derechos como el derecho a la vivienda, su derecho al libre movimiento, identidad cultural y el derecho a la protección contra el desplazamiento arbitrario.

102 **Gobierno de Israel**. "Israel y Marruecos firman un histórico Memorando de Entendimiento en Defensa." 24 de noviembre de 2021.
Disponible en:
https://www.gov.il/en/pages/israel-and-morocco-sign-historic-defense-mou-24-november-2021.

103 **Diaride Girona**. "Una empresa israelí abrirá una fábrica de drones en Marruecos." 28 de abril de 2024.
Disponible en:
https://www.diaridegirona.cat/economia/2024/04/28/empresa-israeli-abrira-fabrica-drones-101651241.html.

III

TÚNEZ: EL ESTADO DE EMERGENCIA PERMANENTE

Durante las dos décadas en que Túnez fue gobernada por el autócrata Zine el Abidine Ben Ali, derrocado en 2011, el Gobierno extendió su vigilancia a los espacios privados de la población, a través de un aparato de seguridad particularmente invasivo. Tras la caída del régimen después de la Revolución del Jazmín de 2011, la situación pareció revertirse y creció el uso de la tecnología para controlar al poder, por ejemplo, a través de la dinámica de llevar cámaras a las manifestaciones y protestas para grabar los abusos policiales[104]. Fue entonces cuando también salió a la luz el mecanismo de cibervigilancia con el que la Agencia Tunecina de Internet del Gobierno de Ben Ali había estado censurando blogs y medios críticos con el poder, conocido como Ammar 404[105], que se convirtió en el símbolo de la vigilancia masiva durante la dictadura.

Casi quince años después, Túnez es hoy un país en estado de emergencia permanente, que reaprovecha parcialmente la arquitectura legal y tecnológica de la dictadura para continuar vigilando y reprimiendo a juezas, periodistas, abogadas, sindicalistas, oposición política y activismo LGBTIQ+, a través de leyes antiterroristas y contra la ciberdelincuencia[106]. Si bien Túnez ha permanecido en el Índice de Libertad de Prensa de Freedom House como el país árabe más garantista, la propia organización reconoce, en su informe anual de 2023, que la población tunecina es perseguida por publicar en la red contenido crítico con el presidente, el Gobierno o las fuerzas de seguridad[107].

1. RECUPERANDO LAS ESTRUCTURAS DE VIGILANCIA DIGITAL DE LA DICTADURA

Durante los últimos años del régimen de Ben Ali, convivieron dos tendencias paralelas: el aumento del acceso a internet de la población tunecina y un control férreo de las comunicaciones, simbolizado por Ammar 404. Este era el mensaje de error que aparecía cuando se intentaba acceder, desde el interior del país a una de las numerosas páginas web censuradas, entre ellas los medios Al Jazeera, Al Arabiya y medios digitales tunecinos críticos

104 **Cheikh, Mériam y Pluta, Audrey**. "L'ordre et la force. Police, sécurité et surveillance au Nord de l'Afrique", L'Année du Maghreb. 2023
Disponible en: https://journals.openedition.org/anneemaghreb/12646

105 **Webdo TN**. «Tunisie: Qui se cachait derrière Ammar 404 ?» 31 de enero de 2011.
Disponible en: https://www.webdo.tn/fr/actualite/national/qui-se-cachait-derriere-ammar-404/173718.

106 **Amnistía Internacional.** "Túnez." Consultado el 25 de octubre de 2024.
Disponible en: https://www.es.amnesty.org/en-que-estamos/paises/pais/show/tunez/.

107 **Informe Freedom in the World 2023**. Freedom House.
Disponible en: https://freedomhouse.org/country/tunisia/freedom-world/2023

como Nawaat[108] [109]. Este sistema se encargaba de vigilar a blogueras y periodistas críticas con las autoridades. Los correos electrónicos de la disidencia política eran interceptados de forma sistemática usando tecnologías de inspección profunda de paquetes (DPI)[110] [111], que el Gobierno tunecino habría obtenido de las empresas estadounidenses Blue Coat System y Netapp, y de la alemana Utimaco, según hicieron público posteriormente defensoras de derechos humanos[112]. Por otro lado, Trovicor, antigua subsidiaria de Siemens AG y Nokia Siemens, con sede en Múnich, habría proporcionado al Gobierno tecnologías que permiten su uso para la intercepción de voz y datos, así como la mejora de las herramientas para llevar a cabo escuchas[113]. Sundby ETI A/S, empresa danesa, subsidiaria de BAE Systems, habría vendido, según Privacy International, tecnología de intercepción de datos de teléfonos móviles capaz de trackear[114] los hábitos de navegación de las usuarias y realizar registros de correos electrónicos[115].

Tras la caída del autócrata en 2011, la Agencia Tunecina de Internet (ATI), promotora del desarrollo de la red en el país, pasó a ser dirigida por Moez Chakchouk, que dio por desmantelado el aparato de vigilancia digital del régimen y lo reemplazó por una política de apertura y democratización del acceso a la red[116]. Sin embargo, la dinámica de cambio no duró mucho. En 2013, se constituyó la Agencia para las Telecomunicaciones (ATT), que opera bajo el mando del Ministerio de Comunicaciones y Tecnologías de la Información y que "provee de apoyo técnico a las investigaciones judiciales sobre delitos relacionados con la comunicación"[117]. Activistas de internet como Afef Abrougui ya advirtieron entonces de que se estaba recuperando el pretexto de la lucha contra el terrorismo para controlar la

108 **Swissinfo**. "La primavera árabe: la primera revolución smartphone." 21 de enero de 2020. https://www.swissinfo.ch/spa/la-primavera-%C3%A1rabe-la-primera-revoluci%C3%B3n-smartphone/46193332.

109 **Ben Mhenni, Lina.** "Tunisia: 404 not found." Global Voices Advox. 24 de septiembre de 2008. Disponible en: https://advox.globalvoices.org/2008/09/24/tunisia-404-not-found

110 Ver glosario.

111 **Privacy International**. "State surveillance in Tunisia." 2019. Disponible en: https://www.privacyinternational.org/state-privacy/1012/state-surveillance-tunisia

112 **Goupy, Marie**. «La bienveillante neutralité des technologies d'espionnage des communications : le cas tunisien.» Cultures & conflits, n.º 93. 8 de julio de 2014. Disponible en: https://journals.openedition.org/conflits/18863

113 **Timm, Trevor**. "Spy Tech Companies & Their Authoritarian Customers, Part II: Trovicor and Area SpA", Electronic Frontier Foundation. 21 de febrero de 2012. Disponible en: https://www.eff.org/deeplinks/2012/02/spy-tech-companies-their-authoritarian-customers-part-ii-trovicor-and-area-spa

114 "Trackear" es un término que proviene del inglés "to track" y se refiere al acto de seguir, monitorear o registrar la ubicación, el comportamiento o la actividad de algo o alguien.

115 **Privacy International**. "State of surveillance, Tunisia." 14 de marzo de 2019. https://privacyinternational.org/state-privacy/1012/state-surveillance-tunisia.

116 **El Dahshan, Mohamed**. "Hacking in Ben Ali's Basement". Foreign Policy, 26 de junio de 2013. Disponible en: https://foreignpolicy.com/2013/06/26/hacking-in-ben-alis-basement/

117 Decreto 2013-4506 aprobado el 6 de Noviembre de 2013. Artículo 2.

"La ausencia de transparencia en la compra pública de tecnología no permite saber con exactitud qué tecnologías de vigilancia del régimen de Ben Ali están siendo utilizadas"

información en la red[118]. El retorno a las dinámicas de vigilancia y control del gobierno anterior se reforzaría en 2015, a raíz de una ola de atentados contra turistas perpetrados por el autodenominado Estado Islámico[119]. Poco después se aprobó la Ley 2015/26 de Lucha Contra el Terrorismo, duramente criticada por organizaciones de derechos humanos locales e internacionales, que consideraban que el nuevo decreto abría la puerta de nuevo al monitoreo y a la vigilancia masiva[120]. Ese año se declaró, también, el estado de emergencia, que ha continuado vigente durante la última década. La ausencia de transparencia en la compra pública de tecnología no permite saber con exactitud qué tecnologías de vigilancia del régimen de Ben Ali han seguido siendo utilizadas por los gobiernos posteriores y en la actualidad[121].

2. COTO A LA LIBERTAD DE EXPRESIÓN CON EL PRETEXTO DE LA CIBERDELINCUENCIA Y LAS "*FAKE NEWS*"[122]

Desde la llegada del presidente Kaïs Saïed al poder en 2019, el cerco contra defensoras de derechos humanos y voces opositoras al Gobierno se ha intensificado de forma alarmante. En 2020, Amnistía Internacional publicó un informe con los casos de 40 blogueras, administradoras de páginas populares de Facebook y defensoras de derechos humanos que fueron condenadas por cargos como difamación, desacato a las instituciones estatales y "daño" a otros a través de redes sociales. La ONG expresaba su preo-

118 **Abrougui, Afef**. "Tunisians cast a wary eye on new crime agency - Index on Censorship". Index on Censorship, 2 de enero de 2014.
Disponible en: https://www.indexoncensorship.org/2014/01/tunisians-cast-a-wary-eye-on-att/.

119 **BBC News**. "Tunisia attacks: Militants jailed over 2015 terror". 9 de febrero de 2019.
Disponible en: https://www.bbc.com/news/world-africa-47183027

120 **Human Rights Watch**. "Tunisia: Counterterror Law Endangers Rights". 31 de julio de 2015.
Disponible en: https://www.hrw.org/news/2015/07/31/tunisia-counterterror-law-endangers-rights

121 **Privacy International**. "Suggestions for privacy-related questions to be included in the list of issues on Tunisia, Human Rights Committee, 122nd session, March-April 2018".
Disponible en: https://ccprcentre.org/files/documents/INT_CCPR_ICS_TUN_30055_E.pdf

122 Ver glosario.

cupación por la creciente tendencia a comprometer la libertad de expresión en las redes usando la arquitectura legal y punitiva del régimen[123]. Es el caso de la bloguera tunecina Emna Chargui, que posteó en Facebook un texto satírico sobre el COVID-19 y las medidas de confinamiento en forma de versículo del Corán. Además de recibir amenazas de muerte y de violencia sexual (un ataque frecuentemente utilizado contra las mujeres y las personas LGBTIQ+) por parte de personas no identificadas, Chargui fue condenada a seis meses de cárcel por "ofender los sentimientos religiosos", mientras que las amenazas que sufrió no han sido investigadas[124].

Esta tendencia se aceleró de forma dramática en 2021, cuando 60 organizaciones de derechos humanos denunciaron la ola de represión contra defensoras de derechos humanos tunecinas, que incluía: el asesinato de dos personas y alrededor 2.000 detenciones en solo 2 meses, numerosos casos de acoso policial a través de las redes sociales, la condena a 6 meses de cárcel de la activista queer Rania Amdouni o las torturas a jóvenes en comisaría[125]. El presidente Saïed aprovechó el malestar en las calles, en parte catalizado por las restrictivas medidas decretadas durante la pandemia de COVID-19, para congelar la actividad del Parlamento y disolvió el Gobierno, otorgándose plenos poderes constitucionales bajo el argumento de que Túnez estaba al borde de un "peligro inminente"[126].

En 2022, se aprobó una nueva Constitución que preveía la posibilidad de suspender el derecho a la privacidad, recogido en la carta magna de 2014, en caso de que el país se encontrara bajo "estado de emergencia"[127]. Un estado de emergencia que estaba vigente cuando se adoptó el nuevo texto y que se ha alargado mediante decreto hasta diciembre de 2024[128]. Poco después, se aprobó el Decreto Ley núm. 2022-54, de 13 de septiembre de

123 **Amnistía Internacional**. "Tunisia: Criminal Prosecutions of Online Speech: Outdated and Flawed Laws Used to Restrict Speech in Tunisia."
Disponible en: https://www.amnesty.org/en/documents/MDE30/3286/2020/en/"

124 **Amnistía Internacional**. "Tunisia: Blogger Emna Chargui sentenced to six months in prison for social media post." 9 de noviembre de 2020.
https://www.amnesty.org/en/latest/news/2020/07/tunisia-blogger-emna-chargui-sentenced-to-six-months-in-prison-for-social-media-post/#:~:text=On%202%20May,%20Emna%20Chargui,for%20her%20to%20be%20punished.

125 **Nawaat**. "Avec le gouvernement Mechichi, l'Etat policier renaît de ses cendres. 11 de marzo de 2021."
Disponible en:
https://nawaat.org/2021/03/11/avec-le-gouvernement-mechichi-letat-policier-renait-de-ses-cendres/

126 **France 24**. "Tunisie: Le président Kaïs Saïed suspend le Parlement et démet le Premier ministre Hichem Mechichi." 25 de julio de 2021.
Disponible en:
https://www.france24.com/fr/info-en-continu/20210725-tunisie-le-pr%C3%A9sident-ka%C3%AFs-sa%C3%AFed-suspend-le-parlement-et-d%C3%A9met-le-premier-ministre-hichem-mechichi

127 **Privacy International**. "State Surveillance in Tunisia" 2019.
Disponible en: https://www.privacyinternational.org/state-privacy/1012/state-surveillance-tunisia

128 **Europa Press**. "El presidente de Túnez anuncia la ampliación por otro año más del largo estado de emergencia." 21 de enero de 2024.
Disponible en:
https://www.europapress.es/internacional/noticia-presidente-tunez-anuncia-ampliacion-otro-ano-mas-largo-estado-emergencia-20240131024235.html

2022, la llamada 'Ley de Ciberdelincuencia', que castiga la difusión de información falsa de forma malintencionada a través de redes digitales. Esta Ley utiliza términos ambiguos, como el de *fake news*[129], y otorga a las autoridades el poder de cerrar medios de comunicación y organizaciones de la sociedad civil en caso de violación de su articulado[130]. La Ley establece disposiciones para permitir a las autoridades "recoger pruebas electrónicas", recopilar datos personales e interceptar comunicaciones privadas, basándose en criterios vagos. Desde entonces, más de 40 personas han sido detenidas arbitrariamente por su defensa de derechos o libertad de expresión, el grueso de ellas acusadas de "conspiración" bajo la Ley de Ciberdelincuencia. La mayoría llevan meses en prisión preventiva a la espera de juicio, en algunos casos más de un año[131].

"la lucha contra la ciberdelincuencia se focaliza especialmente en personas jóvenes, que en Túnez han sido catalizadoras de movilizaciones importantes tras las Primaveras Árabes, por la falta de perspectivas de empleo y futuro"

Esta represión en nombre de la lucha contra la ciberdelincuencia se focaliza especialmente en personas jóvenes, que en Túnez han sido catalizadoras de movilizaciones importantes tras las Primaveras Árabes, por la falta de perspectivas de empleo y futuro. Uno de los casos más conocidos es el del estudiante Ahmed Hamada, que administraba una página de Facebook donde se publicaban los abusos policiales contra el vecindario de clase trabajadora del barrio Hay Tadhamon, en la capital. Hamada fue detenido en octubre de 2022 y su ordenador y su teléfono móvil fueron requisados para la extracción de datos. Se enfrenta a 12 años de cárcel por "utilizar sistemas de comunicación para expandir intencionalmente *fake news* contra agentes del Estado"[132].

129 Ver glosario.

130 **Amnistía Internacional.** "La Tunisie doit abroger le décret relatif à la cybercriminalité." 12 de diciembre de 2022. Disponible en: https://www.amnesty.org/es/documents/mde30/6290/2022/fr»

131 **Human Rights Watch.** "Tunisie : Un décret sur la cybercriminalité utilisé contre les détracteurs des autorités." 19 de diciembre de 2023.
Disponible en:
https://www.hrw.org/fr/news/2023/12/19/tunisie-un-decret-sur-la-cybercriminalite-utilise-contre-les-detracteurs-des»

132 **The International Commission of Jurists - ICJ.** "Tunisia: Silencing Free Voices." Julio de 2023.
Disponible en:
https://www.icj.org/wp-content/uploads/2023/07/Tunisia-Silencing-Free-Voices-_compressed-1.pdf

3. INTERCEPCIÓN DE COMUNICACIONES Y HACKEO DE DISPOSITIVOS

Además de la Ley de Ciberdelincuencia, la renovación de estado de emergencia en 2023 garantizó a la Agencia Tunecina de Telecomunicaciones (ATT) el acceso a los contenidos de dispositivos electrónicos sin orden judicial[133], confiriéndole plenos poderes para confiscar dispositivos, extraer datos e interceptar comunicaciones.

En febrero de 2024, fueron encausadas 17 personas de partidos de la oposición, funcionarios del Estado y miembros de la iniciativa "Citizens against the coup", -que exige el fin del estado de emergencia, bajo la ley antiterrorista de 2015- acusadas de conspirar para derrocar al presidente Saïed. A algunas de las personas acusadas se les confiscaron teléfonos móviles e incluso tarjetas de almacenamiento, según una investigación del medio crítico Inkyfada, que tuvo acceso al expediente judicial. Durante los interrogatorios, también se utilizaron extractos de conversaciones de WhatsApp, Telegram e incluso de Signal[134], que mantuvieron supuestamente con diplomáticos extranjeros.

Como en el resto de la región, uno de los principales objetivos de la intercepción de comunicaciones en Túnez son las personas LGBTIQ+, donde las prácticas sexuales entre personas del mismo sexo están penadas hasta con 3 años de cárcel[135]. La digitalización de las relaciones en el país ha traído consigo la criminalización de la llamada "inmoralidad digital", que se ha materializado en la hipervigilancia y la exposición de datos e información íntima de decenas de personas LGBTIQ+[136]. Una de las tendencias crecientes en este sentido es la extracción de información de dispositivos, sea mediante acceso no consentido, hacking o amenazas. Human Rights Watch relata el caso de una pareja de hombres que fueron interrogados sobre su activismo LGBTIQ+ por agentes de policía, que les exigieron ver sus conversaciones y páginas de Facebook. A pesar de haberse negado a ello, los agentes les confesaron que, en realidad, ya habían accedido a esa información gracias a su casero, que dio el consentimiento para acceder a su wifi y hackear sus cuen-

133 **Freedom House**. 2023. Disponible en: https://freedomhouse.org/country/tunisia/freedom-world/2023

134 **Issa, Ziadia**. "Enquête | "Complot contre la sûreté de l'État": des dossiers vides pour éliminer l'opposition.» inkyfada.com. 24 de marzo de 2023.
Disponible en: https://inkyfada.com/fr/2023/03/24/complot-surete-etat-dossiers-opposition-tunisie/.

135 **Human Dignity Trust**. "Tunisia | Human Dignity Trust."
Disponible en:
https://www.humandignitytrust.org/country-profile/tunisia/#:~:text=Article%20230%20criminalises%20'sodomy'%20between,men%20and%20also%20between%20women.

136 **Human Rights Watch**. «Tunisie : Arrestations arbitraires d'activistes LGBTI et violences policières.» 23 de febrero de 2021.
Disponible en:
https://www.hrw.org/fr/news/2021/02/23/tunisie-arrestations-arbitraires-dactivistes-lgbti-et-violences-policieres.

tas de correo, sus teléfonos y sus ordenadores portátiles[137], recopilando gran cantidad de información privada.

Además, el activismo LGBTIQ+ se enfrenta a los ataques de trolls o ejércitos electrónicos[138], organizados en las redes sociales, donde se les denigra y se incita a la violencia contra ellas. En 2021, un grupo de defensoras de derechos humanos que enarbolaron la bandera arcoíris en una manifestación en Túnez capital fue sometido a acoso online, en algunos casos por parte de páginas de Facebook asociadas a sindicatos policiales. Es el caso de la artista lesbiana Rania Amdouni, de quien circularon cientos de fotografías con amenazas de muerte y cuya dirección y número de teléfono fueron filtrados por trolls[139] [140]. En algunos casos, estas personas llegan a huir del país por la inseguridad que sienten (sexilio).

4. INVERSIÓN OCCIDENTAL MILLONARIA PARA LA VIGILANCIA DE FRONTERAS

Buena parte de la tecnología más sofisticada que se utiliza desde el Gobierno se vehicula hacia la vigilancia de la costa tunecina y de la frontera con Libia, con el objetivo de controlar no solo la migración a Europa, sino también la presencia de grupos islamistas violentos, sobre todo después de los ataques de 2015. De 2016 a 2018, el Gobierno construyó un muro de 200 kilómetros a lo largo de su frontera con Libia, equipado con sistemas de alta resolución y alcance de larga distancia, cámaras térmicas y con detección de movimiento, vinculadas a una central de vigilancia. El proyecto fue financiado por Alemania[141] y Estados Unidos[142],

137 **Human Rights Watch**. "All This Terror Because of a Photo." 2023. https://www.hrw.org/sites/default/files/media_2023/03/lgbt_mena0223web.pdf.

138 Ver glosario.

139 **Coda Stor**y. "Tunisian Police Are Using Drones and Facebook to Doxx LGBTQ Protesters." 22 de abril de 2021. https://www.codastory.com/authoritarian-tech/anti-lgbt-crackdown-in-tunisia.

140 Ver glosario.

141 **Webdo.** "Des équipements de surveillance électronique allemands à la Tunisie." 16 de octubre de 2024. https://www.webdo.tn/fr/actualite/national/lallemagne-remettra-bientot-equipements-de-surveillance-electronique-a-tunisie/163767.

142 **Kapitalis**, Webmaster. "Des Américains installent la surveillance électronique au sud de la Tunisie," 14 de agosto de 2016. Disponible en: https://kapitalis.com/tunisie/2016/08/14/des-americains-installent-la-surveillance-electronique-au-sud-de-la-tunisie.

“La dinámica de coartar libertad de movimiento y de salida del país a las personas que migran desde Túnez se ha agravado en los últimos años, acompañado por campañas racistas de acoso y difamación en redes”

y lo ejecutó URS, filial de la multinacional de ingeniería AECOM, ambas estadounidenses [143] [144].

Recientemente, el Gobierno ha adquirido un sofisticado sistema de reconocimiento digital e identificación biométrica proporcionado por el gigante francés Idemia[145]. La justificación para poner en marcha estos sistemas es reforzar las capacidades técnicas y operacionales en seguridad de fronteras y la persecución de grupos “terroristas”. La dinámica de coartar libertad de movimiento y de salida del país a las personas que migran desde Túnez se ha agravado en los últimos años, acompañado por campañas racistas de acoso y difamación en redes, alimentadas por el propio presidente Saïed[146]. También se ha denunciado violencia, incluyendo violencia sexual contra las mujeres migrantes, como publicaba recientemente The Guardian[147]. Desde 2013, el Ministerio del Interior tunecino ha impuesto restricciones de circulación a casi 30.000 personas en virtud de las medidas de control de las fronteras, que no son públicamente accesibles y carecen por completo de supervisión judicial, tal y como denunciaba Amnistía Internacional en un informe publicado en 2018[148].

143 Ibid.

144 **Webdo**. “Le système de surveillance électronique à la frontière tuniso-libyenne». Disponible en: https://www.webdo.tn/fr/actualite/national/systeme-de-surveillance-electronique-a-frontiere-tuniso-libyenne-installe-2018/158669

145 **Actu-Maroc**, “Kaïs Saied lance un programme de sécurité numérique en Tunisie malgré la crise économique,”. 1 de marzo de 2024. Disponible en: https://www.actu-maroc.com/kais-saied-lance-un-programme-de-securite-numerique-en-tunisie-malgre-la-crise-economique/.

146 **Amnistía Internacional**. “El discurso racista del presidente de Túnez incita una ola de violencia contra africanos negros.” Publicado el 14 de marzo de 2023. https://www.amnesty.org/en/latest/news/2023/03/tunisia-presidents-racist-speech-incites-a-wave-of-violence-against-black-africans/

147 **The Guardian**, “The brutal truth behind Italy’s migrant reduction: beatings and rape by EU-funded forces in Tunisia,” 19 de septiembre de 2024. Disponible en: https://www.theguardian.com/global-development/2024/sep/19/italy-migrant-reduction-investigation-rape-killing-tunisia-eu-money-keir-starmer-security-forces-smugglers

148 **Amnistía Internacional**, “Túnez: Restricciones de viajar arbitrarias y abusivas vulneran los derechos humanos,” 24 de octubre de 2018. Disponible en: https://www.amnesty.org/es/latest/press-release/2018/10/tunisia-arbitrary-and-abusive-travel-restrictions-breach-human-rights/

IV

EGIPTO: EL ESTADO COMO HACKER MALICIOSO Y ACOSADOR ONLINE

Cuando la Primavera Árabe llegó a la plaza Tahrir de El Cairo en 2011, el Gobierno de Mubarak amplió la tecnología disponible para interceptar llamadas de teléfono y estrechar el cerco contra las defensoras de derechos humanos que luchaban contra el régimen. En 2016, un informe de Privacy International desvelaba la existencia de una unidad secreta, el Departamento de Investigación Técnica (TRD, por sus siglas en inglés), atribuida al Servicio General de Inteligencia egipcio, que habría adquirido tecnología de vigilancia de la finlandesa Nokia Siemens Network[149]. Tras el golpe militar del presidente del Consejo Supremo de las Fuerzas Armadas, Abdul Fatah al-Sisi, contra el entonces presidente electo surgido tras las revueltas Mohamed Morsi en 2013, la situación no sólo no mejoró por lo que respecta a la libertad de expresión y a los derechos políticos, sino que la libertad en Internet y los derechos de los usuarios fueron severamente restringidos, como señala el informe *Freedom on the Net* de 2023[150]. Las sanciones penales, el acoso y la vigilancia han contribuido a convertir el periodismo crítico con el Gobierno en una actividad imposible, impulsando la censura y la autocensura.

A su vez, las agencias egipcias de seguridad han adquirido de empresas occidentales sofisticada tecnología para el espionaje, el control y la intercepción de las comunicaciones, dinámica que han llevado a cabo de forma extremadamente exhaustiva, mientras desarrollaban una industria propia de la vigilancia[151]. La censura masiva de páginas web, que se calcula en más de 600 sitios bloqueados desde 2017, y la persecución y acoso a periodistas, defensoras de derechos humanos y personas LGBTIQ+, han convertido el país norteafricano en un cliente prolífico y un auténtico laboratorio para las tecnologías de vigilancia masiva y monitoreo online de empresas occidentales.

149 **Privacy International.** "The President's Men." 2016.
https://www.privacyinternational.org/sites/default/files/2018-02/egypt_reportEnglish_0.pdf.

150 **Freedom House.** "Freedom on the Net 2023, Country: Egypt."
Disponible en: https://freedomhouse.org/country/egypt/freedom-net/2023.

151 **Shea, Joey.** "Global Tech and Domestic Tactics: Egypt's Multifaceted Regime of Information Controls." The Tahrir Institute for Middle East Policy. 31 de enero de 2020.
Disponible en:
https://timep.org/2020/01/31/global-tech-and-domestic-tactics-egypts-multifaceted-regime-of-information-controls/.

1. ROBO DE CREDENCIALES Y ACCESO FRAUDULENTO A LAS CUENTAS DE CORREO DE ONG DE DERECHOS HUMANOS

En Egipto, el Gobierno de Al Sisi es extremadamente activo en el acoso digital a la sociedad civil, si se atiende a la cantidad de informes y denuncias de defensoras de derechos humanos que se han hecho públicas en los últimos años. Su acción no se limita a la clásica intercepción de las comunicaciones por aplicaciones de mensajería o telefónicas, sino que utiliza todos los medios a su alcance. En 2017, salió a la luz una campaña de *phishing*[152] llamada "Nile Phish" ("Pez del Nilo") contra al menos siete ONG de derechos humanos y defensoras de derechos humanos, abogadas y periodistas del país[153]. Según una investigación de la organización Citizen Lab, el uso de esta técnica informática resultó en el hackeo de docenas de cuentas de Gmail y Dropbox[154]. En este caso, las víctimas se infectaron a través de un falso correo de la organización Nadeem Center for Rehabilitation of Victims of Violence (clausurada por las autoridades egipcias desde entonces) e invitaba a abrir un enlace para obtener más información sobre una supuesta conferencia. El ataque fue orquestado usando una plataforma de fuente abierta y gratuita llamada GoPhish, que permite crear simulaciones realistas de usuarios fiables.

"el Gobierno de Al Sisi es extremadamente activo en el acoso digital a la sociedad civil"

En marzo de 2019, una investigación de Amnistía Internacional desveló otra oleada de ataques digitales que "probablemente se originaron por organismos respaldados por el Gobierno"[155] y que implicó múltiples intentos de obtener acceso a las cuentas de correo electrónico de varias defensoras de derechos humanos, medios de comunicación y personal de organizaciones egipcias. Esta nueva campaña se producía en medio de lo que la ONG consideraba una "ofensiva sin precedentes que ha convertido a Egipto en una

152 Ver glosario.

153 **Withaker, Bryan.** "How the Middle East Became an Electronic Battleground." Hackernoon. 19 de junio de 2017. Disponible en: https://hackernoon.com/how-the-middle-east-became-an-electronic-battleground-dac5b5435eb.

154 **Scott-Railton, John; Marczak, Bill; Raoof, Ramy; y Maynier, Etienne.** "Nile Phish: Large-Scale Phishing Campaign Targeting Egyptian Civil Society." Citizen Lab. 2017. Disponible en: https://citizenlab.ca/2017/02/nilephish-report/?ref=hackernoon.com.

155 **Amnesty International.** "Phishing attacks using third-party applications against Egyptian civil society organizations". 6 de marzo de 2019. Disponible en: https://www.amnesty.org/en/latest/research/2019/03/phishing-attacks-using-third-party-applications-against-egyptian-civil-society-organizations/

prisión 'al aire libre' para los críticos"[156]. En este caso, los atacantes no recurrieron a métodos tradicionales de *phishing*[157] para robar credenciales, sino que utilizaron una forma más sigilosa y eficiente de acceder a las bandejas de entrada de las víctimas: una técnica conocida como *OAuth Phishing*[158], que engaña a las usuarias para que otorguen permisos a aplicaciones maliciosas que pueden acceder a los datos de su cuenta y realizar acciones en su nombre. Básicamente, los atacantes engañaron a las víctimas para que les concedieran acceso total a sus correos electrónicos, a través de aplicaciones móviles alojadas en la Play Store oficial de Google y Android[159].

"los atacantes engañaron a las víctimas para que les concedieran acceso total a sus correos electrónicos, a través de aplicaciones móviles alojadas en la Play Store oficial de Google y Android"

Según un informe publicado meses después por Check Point Research, plataforma de inteligencia de la empresa israelí CheckPoint Software Technologies, el ataque afectó a 33 periodistas, políticas, abogadas y defensoras de derechos humanos, cuyos correos, contactos y localización fueron interceptados y registrados[160]. CheckPoint no encontró una relación directa e irrefutable con los servicios de inteligencia egipcios, aunque la plataforma consideró que dados "los objetivos, la clara intención y propósito de las aplicaciones, la estructura y los datos descargados, así como un servidor registrado en el Ministerio de Tecnologías de la Información y una ubicación codificada que corresponde a la sede de la principal agencia de espionaje de Egipto, es casi seguro que se trató de una acción impulsada por el Gobierno"[161].

156 Ibid.

157 Ver glosario.

158 Ver glosario.

159 **Checkpoint Research.** "The eye on the Nile." 2019.
Disponible en: https://research.checkpoint.com/2019/the-eye-on-the-nile/.

160 **Checkpoint Research.** "The eye on the Nile." 2019.
Disponible en: https://research.checkpoint.com/2019/the-eye-on-the-nile/.

161 Ibid

2. ESPIONAJE Y EXTRACCIÓN DE DATOS CON TECNOLOGÍA Y CAPITAL ISRAELÍ

Entre mayo y septiembre de 2023, el exparlamentario egipcio Ahmed Eltantawy fue objeto de varios intentos de infección de su teléfono móvil con el *spyware*[162] Cytrox's Predator, tras anunciar su intención de presentarse a las elecciones presidenciales de 2024[163]. Este tipo de programa permite el monitoreo de los aparatos infectados, independientemente de su localización, en tiempo real[164]. Cytrox forma parte de Intellexa Consortium, un grupo de empresas de *spyware*[165] y servicios relacionados conocida por competir con NSO Group y vender tecnología a aquellos países a los que NSO ya no vende sus productos tras escándalos relacionados con su impacto en vulneraciones de derechos humanos[166]. En marzo de 2024, el Departamento del Tesoro estadounidense sancionó a Cytrox y a Intellexa Consortium por vender herramientas de espionaje y vigilancia masiva a regímenes autoritarios y "por su rol en el desarrollo y distribución de *spyware*[167] usado contra ciudadanos estadounidenses, incluyendo miembros del Gobierno, periodistas y asesores"[168].

La conexión móvil de Eltantawy fue atacada de forma persistente mediante inyección de red[169]. Cuando visitaba determinados sitios web que no utilizaban HTTPS, un dispositivo instalado en la frontera de la red de Vodafone Egipto le redirigía automáticamente a un sitio web malicioso para infectar su teléfono con el programa espía, a la vez que recibía enlaces por SMS y Whatsapp para facilitar que cayera en la trampa. El exparlamentario, que sospechaba que podía estar siendo víctima de un intento de infección, contactó con

162 Ver glosario.

163 **Attalah, Lina.** "Aspiring presidential candidate Ahmed Tantawi targeted by Predator spyware", *Mada.* 14 de septiembre de 2023.
https://www.madamasr.com/en/2023/09/14/news/u/aspiring-presidential-candidate-ahmed-tantawi-targeted-by-predator-spyware/

164 **Sekoia.io.** "Predator spyware." Disponible en: https://www.sekoia.io/en/glossary/predator-spyware/.

165 Ver glosario.

166 **Red en Defensa de los Derechos Digitales.** "Estados Unidos sanciona al CEO de Intellexa, empresa creadora de spyware, por violaciones de Derechos humanos."
Disponible en:
https://r3d.mx/2024/03/20/estados-unidos-sanciona-al-ceo-de-intellexa-empresa-creadora-de-spyware-por-violaciones-a-derechos-humanos/.

167 Ver glosario.

168 **US Department of Treasury.** "Treasury Sanctions Members of the Intellexa Commercial Spyware Consortium". 05 de marzo de 2024.
Disponible en: https://home.treasury.gov/news/press-releases/jy2155.

169 Ver glosario.

la plataforma Citizen Lab.[170] En el comunicado en el que confirmaba las sospechas de Eltantawy, Citizen Lab aseguraba que "dado que Egipto es un cliente conocido del programa espía Predator de Cytrox, y que el programa espía se entregó a través de inyección de red[171] desde un dispositivo ubicado físicamente dentro de Egipto, atribuimos el ataque de inyección de red al Gobierno egipcio con alta probabilidad".[172] Durante ese mismo período, las fuerzas de seguridad detuvieron a varias personas voluntarias de su campaña política[173].

3. TECNOLOGÍA CANADIENSE PARA LA CENSURA DE PÁGINAS WEB CRÍTICAS

La censura de páginas web a gran escala, además de una tendencia regional, es también una dinámica destacada en el contexto egipcio. Desde 2017, más de 600 sitios y dominios son inaccesibles desde el interior del país. Este fenómeno lo han denunciado en 2020 organizaciones egipcias, regionales e Internacionales como Cairo Institute for Human Rights Studies (CIHRS) o la Electronic Frontier Foundation (EFF), que señalaron que esa dinámica constituiría una violación del derecho al acceso a la información y a la libertad de

"La censura de páginas web a gran escala, además de una tendencia regional, es también una dinámica destacada en el contexto egipcio. Desde 2017, más de 600 sitios y dominios son inaccesibles desde el interior del país"

170 **Scott-Railton, John et al.** "Pegasus vs. Predator. Dissident's Doubly-Infected iPhone Reveals Cytrox Mercenary Spyware". Citizenlab. 16 de diciembre de 2021.
Disponible en:
https://citizenlab.ca/2021/12/pegasus-vs-predator-dissidents-doubly-infected-iphone-reveals-cytrox-mercenary-spyware/

171 Ver glosario.

172 **Scott-Railton, John et al.** "Predator in the wires. Ahmed Eltantawy Targeted with Predator Spyware After Announcing Presidential Ambitions". Citizenlab. 22 de septiembre de 2023.
Disponible en:
https://citizenlab.ca/2023/09/predator-in-the-wires-ahmed-eltantawy-targeted-with-predator-spyware-after-announcing-presidential-ambitions/

173 **Mada.** "Presidential hopeful Ahmed Tantawi: Friends 'disappeared' before reaching campaign HQ". 28 de mayo de 2023.
Disponible en:
https://www.madamasr.com/en/2023/05/28/news/u/presidential-hopeful-ahmed-tantawi-friends-disappeared-before-reaching-campaign-hq/.

expresión[174]. Las webs pertenecen a medios de comunicación críticos, plataformas políticas y de denuncia de vulneraciones de derechos humanos, como el medio de periodismo social Al Manassa, que ha sufrido persecución y bloqueo desde poco después de su creación en 2016[175]. Las autoridades egipcias han incluso bloqueado los dominios alternativos a los que recurrió el sitio para seguir operando. En junio de 2020, las fuerzas de seguridad allanaron las oficinas de Al-Manassa(176) y arrestaron a la editora en jefe, Nora Younis, quien fue detenida durante tres días bajo cargos de operar un sitio sin licencia y cometer delitos cibernéticos antes de ser liberada bajo fianza. Younis se convirtió en la primera periodista egipcia en enfrentar acusaciones bajo la ley de delitos cibernéticos, a pesar de que Al-Manassa había presentado una solicitud de licencia y pagado las tarifas correspondientes en 2018 [176] [177] [178] [179].

La restricción de acceso a determinados contenidos y el cierre de webs se llevó a cabo apelando a la Ley de Regulación de Medios y Prensa y a la Ley de Delitos Cibernéticos aprobada en 2018, que expande los poderes para la vigilancia online, el bloqueo de webs, la intercepción de comunicaciones y el monitoreo de internet[180]. El artículo 7 de la Ley de Delitos Cibernéticos otorga a la autoridad investigadora el poder de cerrar un sitio web siempre que considere que el contenido constituye un delito o una amenaza a la seguridad nacional o la economía.

---

174 **Arabic Network for Human Rights Information (ANHRI).** "Human rights organizations call on Egypt's government to end internet censorship and website blocking", Ifex,org. 4 de noviembre de 2021. Disponible en: https://ifex.org/human-rights-organizations-call-on-egypts-government-to-end-internet-censorship-and-website-blocking/

175 **Business & Human Rights Resource Centre.** "Egypt: Authorities allegedly use DPI technology to block VPN use." Disponible en: https://www.business-humanrights.org/fr/derni%C3%A8res-actualit%C3%A9s/egypt-authorities-use-dpi-technology-to-block-vpn-use/

176 **Qurium.** "Nora Younis: 'We Always Expect the Police to Come Back to Our Office.'" Qurium Media Foundation. Diciembre de 2021. Disponible en: https://www.qurium.org/fighters/nora-younis-we-always-expect-the-police-to-come-back-to-our-office/

177 **CPJ Middle East**. "Al-Manassa Editor Nora Younis on Censorship in Egypt." Committee to Protect Journalists. 26 de octubre de 2020. Disponible en: https://cpj.org/2020/10/al-manassa-editor-nora-younis-on-censorship-in-egypt/

178 **MPC Journal**. "Egypt Arrests Another Independent Media Journalist." Middle East Politics and Culture Journal. 25 de junio de 2020. Disponible en: https://mpc-journal.org/egypt-arrests-another-independent-media-journalist/

179 **The Street Journal**. "Egypt: Al-Manassa Editor Nora Younis on Censorship in Egypt." The Street Journal. 25 de junio de 2020. Disponible en: https://thestreetjournal.org/egypt-al-manassa-editor-nora-younis-on-censorship-in-egypt/

180 **Ben-Hassine, Wafa.** "Egyptian Parliament Approves Cybercrime Law Legalizing Blocking of Websites and Full Surveillance of Egyptians". Access Now. 20 de junio de 2018. Disponible en: https://www.accessnow.org/egyptian-parliament-approves-cybercrime-law-legalizing-blocking-of-websites-and-full-surveillance-of-egyptians

Al Manassa solicitó los servicios de análisis forense digital de la ONG sueca Qurium[181], dedicada a la defensa de los derechos digitales, protección de datos y la seguridad en Internet, cuya investigación reveló que los proveedores de internet egipcios usan una tecnología llamada inspección profunda de paquetes (DPI)[182] para restringir el acceso a determinados contenidos y páginas web. Según el medio digital tecnológico estadounidense *The Verge*, la inspección profunda de paquetes es una de las tecnologías más invasivas que un país puede usar en su red de Internet. "Esta técnica, empleada por regímenes autoritarios desde Rusia hasta Bahréin, permite a los Gobiernos examinar el contenido del tráfico web a medida que se desplaza por la red, lo que les permite censurar sitios web en tiempo real y realizar una vigilancia detallada de las actividades de la sociedad civil en la red. También requiere un equipo sofisticado, que normalmente proporciona una empresa occidental"[183], afirma el medio digital.

En este caso, la empresa fue Sandvine[184], una compañía canadiense que desde 2017 y hasta agosto de 2024 era propiedad del grupo inversor Francisco Partners, también accionista de NSO Group hasta 2019. En febrero de 2024 se hizo público que el Departamento del Tesoro de Estados Unidos había incluido a Sandvine en una lista por la implicación de su tecnología DPI[185] en la censura online y el espionaje a defensoras de derechos humanos en Egipto[186]. Tras el escándalo, Francisco Partners decidió prescindir de Sandvine y actualmente está en venta por 450 millones de dólares[187].

181 **Qurium**. "How Operators Use Sandvine to Block Independent Media in Egypt." Qurium Media Foundation. 7 de septiembre de 2020. Disponible en: https://www.qurium.org/press-releases/how-operators-use-sandvine-to-block-independent-media-in-egypt/

182 Ver glosario.

183 **Brandom, Russell.** "Egypt Launches Deep-Packet Inspection System". The Verge. 17 de septiembre de 2014. Disponible en: https://www.theverge.com/2014/9/17/6350191/egypt-launches-deep-packet-inspection-with-help-from-an-american

184 **Lyons, Jessica.** "Sandvine Put on America's Export No-Fly List after Egypt Used Network Tech for Spying." The Register. 27 de febrero de 2024. Disponible en: https://www.theregister.com/2024/02/27/

185 Ver glosario.

186 **United States Department of State.** "The United States Adds Sandvine to the Entity List for Enabling Human Rights Abuses." el 28 de febrero de 2024. Disponible en: https://www.state.gov/the-united-states-adds-sandvine-to-the-entity-list-for-enabling-human-rights-ab

187 **Gallagher, Ryan**. "Francisco Partners Ends Ownership of Crisis-Plagued Sandvine". BNN Bloomberg. 23 de agosto de 2024. Disponible en: https://www.bnnbloomberg.ca/business/company-news/2024/08/23/francisco-partners-ends-ownership-of-crisis-plagued-sandvine/.

4. CAMPAÑAS COORDINADAS DE ACOSO Y EMBOSCADAS DIGITALES[188] CONTRA DEFENSORAS DE DERECHOS HUMANOS

Otro de los mecanismos de vigilancia utilizado habitualmente contra defensoras de derechos humanos es el acoso en redes sociales, a menudo alimentado con bots. Este asedio suele intensificarse en momentos puntuales donde la atención mediática está centrada en Egipto y el régimen no puede permitirse que la situación de autoritarismo asfixiante se difunda más allá de sus fronteras.

"En diciembre de 2020, la red X se llenó de contenido homófobo y deshumanizador, viralizado por centenares de trolls y bots, contra el director de la Egyptian Initiative for Personal Rights, Hossam Bahgat"

En diciembre de 2020, un hashtag denigrante contra el director de la Egyptian Initiative for Personal Rights (EIPR), Hossam Bahgat, se hizo viral en el país, llenando la red X (antes Twitter) de contenido homófobo y deshumanizador. El ataque, seguido por centenares de trolls[189] y bots, algunos de ellos progobierno[190] formaba parte de una ofensiva más amplia contra el personal de esta organización de defensa de los derechos humanos egipcia. Tres de los miembros de esta ONG fueron detenidos en el mismo período, tras una visita de 13 diplomáticos a la sede de la organización, y liberados dos días más tarde[191].

No fue este el único método de acoso contra Bahgat. En enero de 2019, tras realizar un tweet crítico, cientos de cuentas falsas comenzaron a seguir su cuenta en X cada minuto durante un par de días. Lejos de ser inocua, esa técnica de ataque generalmente conduce al cierre o suspensión de la cuenta porque se asocia con el comportamiento de los bots.

En las semanas previas a la cumbre sobre el clima COP27, en 2022, más de 150 personas

188 Ver glosario.

189 Ver glosario.

190 **Heikal, Wafaa**. "Egypt: The Coordinated Online Abuse Campaign against EIPR's Founder Hossam Bahgat". Medium. 30 de diciembre de 2020.
Disponible en:
https://wafheikal.medium.com/the-coordinated-harassment-campaign-against-hossam-bahgat-49e95d07dc7d.

191 **FrontLine Defenders.** "Crackdown on Egyptian initiative for personal rights staff.
Disponible en: https://www.frontlinedefenders.org/en/case/crackdown-egyptian-initiative-personal-rights-staff

fueron detenidas e investigadas por la Fiscalía Superior de Seguridad del Estado egipcio por usar las redes sociales para convocar a las protestas contra la cumbre[192]. Se publicó, además, que la aplicación móvil de la COP27, desarrollada por el Ministerio de Comunicaciones y Tecnologías de la Información egipcio, permitía a las autoridades escuchar conversaciones, acceder a correos privados y rastrear mensajes, incluyendo aquellos cifrados[193]. La aplicación fue tildada de "ciber arma", aunque no se pudo demostrar que esta vigilancia se estuviera produciendo.

Como en el resto de la región, pero de forma especialmente violenta en Egipto, las personas LGBTIQ+ continúan siendo un objetivo prioritario para el acoso y la represión online. Desde finales de 2013 hasta 2017, el promedio anual de detenciones fue de 66, mientras que en 2019 fueron 92 las detenciones de personas sospechosas de tener prácticas homosexuales[194]. El uso de aplicaciones de citas como Grindr, Hornet y Growler, habitual en el colectivo LGBTIQ+, se ha convertido en una fuente de riesgo, combinadas con el extremo nivel de vigilancia online y offline. Es el caso de un hombre gay que fue detenido en 2018 durante 11 días, tras tenderle una trampa en la que un oficial de policía le contactó, haciéndole creer que tenía un interés romántico, para después pararlo en un checkpoint y obligarlo a mostrar el contenido de su teléfono móvil[195]. Adicionalmente, tras aprobarse en 2018 la Ley contra los Delitos Cibernéticos, los casos contra personas LGBTIQ+ son juzgados -además de como un agravio a la moralidad- como un delito de cibercrimen, lo que permite a las autoridades imponer sentencias más duras y condenas más estrictas[196].

192 **Coogle, Adam.** "Egypt: Arrests, Curbs on Protests as COP27 Nears". Human Rights Watch. 6 de noviembre de 2022. Disponible en: https://www.hrw.org/news/2022/11/06/egypt-arrests-curbs-protests-cop27-nears

193 **Scott, Mark, y Vincent Manancourt.** "Egypt's COP27 Summit App Is a Cyber Weapon, Experts Warn". POLITICO. el 9 de noviembre de 2022.
Disponible en: https://www.politico.eu/article/cop-27-climate-change-app-cybersecurity-weapon-risks

194 **Afsaneh Rigot.** "Egypt Has a New Tool for Persecuting LGBTQ People," Slate. 30 de diciembre de 2020. Disponible en: https://slate.com/technology/2020/12/egypt-lgbtq-crime-economic-courts.html.

195 **Russell Brandom.** "How LGBTQ Dating Apps Are Unwittingly Aiding Egypt's Crackdown on Gay People," *The Verge*, 25 de abril de 2018.
Disponible en:
https://www.theverge.com/2018/4/25/17279270/lgbtq-dating-apps-egypt-illegal-human-rights.

196 **Afsaneh Right.** "Egypt has a new tool for persecuting LGBTQ people." 30 de diciembre de 2020. Disponible en: https://slate.com/technology/2020/12/egypt-lgbtq-crime-economic-courts.html.

V

LÍBANO: CIBER-ESPIONAJE, CENSURA Y VIOLENCIA DIGITAL EN EL LÍBANO

Las Primaveras Árabes de 2011 en el Líbano sembraron la semilla de la indignación que germinó en nuevos levantamientos populares más sólidos y masivos en años posteriores. Las movilizaciones populares de 2011 demandaban el fin del sistema confesional y sectario en el país. La movilización tan solo duró tres meses[197]. A pesar de ello, la indignación siguió latente y gradualmente emergieron nuevas campañas como en 2013 (#NoToExtension) y en 2015 ("YouStink"). Fue en este marco, donde comenzó a utilizarse el eslogan "All Means All" que daría visibilidad y sentido a las protestas de 2019 contra el Gobierno y el sistema bancario, en la que participaron de forma activa mujeres migrantes y trabajadoras domésticas[198], muchas de las cuales trabajan en el país en un régimen de semiesclavitud[199]. Este proceso representó la emergencia de una nueva generación de defensoras de derechos humanos que combinó de forma hábil las nuevas tecnologías digitales para la organización y la movilización social.

Ante este auge popular, el Gobierno reaccionó reforzando los sistemas de vigilancia masiva. En 2018 salió a la luz pública una sofisticada infraestructura de ciberespionaje, conocida como Dark Caracal, vinculada al Directorio General de Seguridad General libanés (GDGS por sus siglas en inglés) y que desde 2012 había lanzado múltiples campañas de vigilancia masiva con tecnologías avanzadas de empresas occidentales[200]. Los derechos civiles y digitales de la población libanesa están también amenazados, por una parte, debido a un marco regulatorio restrictivo y débil en términos de protección del derecho a la privacidad. Y, por otra parte, por las vulnerabilidades de la infraestructura digital del país como se demostró durante el ciberataque contra la plataforma de registro de pasajeros (MOPHPASS) creada por el Ministerio de Sanidad para la gestión del COVID-19[201]. Más recientemente, el ataque masivo contra buscas y walkie-talkies de militantes de Hezbollah ha demostrado también la capacidad tecnológica de Israel para atacar en territorio libanés[202].

---

197 **Halabi, Fares.** "From Overthrowing the Regime to 'All Means All': An Analysis of the 'Lebanonisation' of Arab Spring Rhetoric." Arab Reform Initiative. 23 de febrero de 2023.
Disponible en:
https://www.arab-reform.net/publication/from-overthrowing-the-regime-to-all-means-all-an-analysis-of-the-lebanonisation-of-arab-spring-rhetoric/

198 **France 24.** "Foreign domestic workers in Lebanon protest abuses." 5 de mayo de 2019.
Disponible en: https://www.france24.com/en/20190505-foreign-domestic-workers-lebanon-protest-abuses

199 **Kvinna till Kvinna**. "Abolishing modern slavery in Lebanon." 27 de marzo de 2023.
Disponible en: https://kvinnatillkvinna.org/2023/03/27/abolishing-modern-slavery-in-lebanon/

200 **The Hacker News.** "Researchers Uncover Government-Sponsored Mobile Hacking Group Operating Since 2012." 19 de enero de 2018.
Disponible en: https://thehackernews.com/2018/01/dark-caracal-android-malware.html.

201 **L'Orient-Le Jour.** "MoPHPass Platform Hacking Problem Has Been Solved, Abiad Says," L'Orient Today. 28 de junio de 2022.
Disponible en:
https://web.archive.org/web/20220629071012/https:/today.lorientlejour.com/article/1290628/mophpass-platform-hacking-problem-has-been-solved-abiad-says.html

202 **ElDiario.es.** "Israel colocó explosivos en miles de beepers importados por Hezbollah y aceleró el ataque por temor a ser descubierto." 18 de septiembre 2024.
Disponible en:
https://www.eldiarioar.com/mundo/israel-coloco-explosivos-miles-buscas-importados-hizbula-acelero-ataque-temor-descubierto_1_11663562.html

1. CIBERESPIONAJE MASIVO A LA POBLACIÓN

En los últimos 20 años, el uso de internet en la sociedad libanesa ha pasado del 9% al 90%[203]. A finales de 2021, alrededor de 4,2 millones de libanesas, aproximadamente el 76% de la población total, eran suscriptores de telefonía móvil[204]. En este contexto, las principales agencias de inteligencia del Líbano como el GDGS, las Fuerzas de Seguridad Internas (ISF) del Ministerio de Interior, y la Dirección de Inteligencia Militar (MID) del Ministerio de Defensa; disponen, cada una, de sus propios sistemas de vigilancia, sobre todo tecnologías para la intercepción de comunicaciones[205]. El MID también dispone de sistemas de monitoreo y extracción de datos de las redes sociales. Además, el MID recibe apoyo del Reino Unido en el marco de la estrategia "Prevent" para luchar contra el extremismo violento[206].

La intercepción de telecomunicaciones es una práctica habitual de las agencias de inteligencia libanesas. En teoría, la Ley 140/1999 sobre Intercepción de Comunicaciones establece que las comunicaciones personales (teléfono, fax, correos electrónicos) están protegidas bajo la ley y que solo pueden ser interceptadas en casos de extrema urgencia y bajo orden judicial o administrativa[207]. Sin embargo, en la práctica estas garantías judiciales no se producen. Según Privacy International, no hay garantías de que los servicios de inteligencia estatales realicen la intercepción de comunicaciones de forma masiva sin ninguna supervisión legal[208]. Desde el asesinato del primer ministro Rafiq Hariri en 2005, las ISF han tenido, en varias ocasiones y bajo autorización del Consejo de Ministros del Líbano acceso ilimitado datos de telecomunicaciones de la sociedad libanesa[209].

Paralelamente, los servicios de inteligencia libaneses han ido adquiriendo tecnologías y servicios de empresas occidentales para la vigilancia masiva de la sociedad civil desde las Primaveras Árabes. En 2015 el MID adquiere por 1,4 millones de dólares, el software de vigilancia masiva "Remote Control System" de la empresa italiana Hacking Team, que permitía grabar audios y tomar capturas de pantalla de móviles, así como monitorear la loca-

203 **DataReportal.** "Digital 2024: Lebanon."
Disponible en: https://datareportal.com/reports/digital-2024-lebanon

204 **CEIC Data.** "Lebanon number of mobile subscribers."
Disponible en: https://www.ceicdata.com/en/indicator/lebanon/number-of-subscriber-mobile

205 Analista digital, entrevista realizada por el equipo de investigación, 9 de septiembre de 2024.

206 **Government of the United Kingdom.** "MENA Lebanon Security Programme Summary FY 18/19."
Disponible en:
https://assets.publishing.service.gov.uk/media/5bf55e3b40f0b60783ad9385/MENA_Lebanon_Security_Programme_Summary_FY_18_19.odt.

207 **Privacy international.** "State of privacy Lebanon." 27 de enero de 2019.
Disponible en: https://privacyinternational.org/state-privacy/1081/state-privacy-lebanon

208 Ibid.

209 Ibid.

lización por GPS de móviles[210]. Asimismo, el centro de investigación de la Universidad de Toronto, Citizen Lab, informó sobre el uso de *spyware*[211] FinFisher de la empresa británica Gamma Group para infectar ordenadores y obtener la información que contienen. Según este centro, las agencias de inteligencia del ISF y el GDGS utilizaron esa tecnología en 2015[212].

"el escaso conocimiento de herramientas de protección digital en el Líbano expone a la sociedad civil a *phishing* y a *spywares* en sus dispositivos móviles

Sin embargo, el mayor sistema utilizado para la vigilancia masiva en el Líbano fue la infraestructura Dark Caracal. En 2018, las organizaciones Lockout y Electronic Frontier Foundation (EFF) publicaron el informe "Dark Caracal. Cyber-espionage at Global Scale" donde se describe un sistema de ciberespionaje masivo con capacidades de Amenazas Persistentes Avanzadas (APT)[213] administrado desde un edificio del GDGS en Beirut desde 2012[214]. Concretamente, Dark Caracal lanzó "campañas de vigilancia" de forma periódica combinando sistemas de hackeo tradicionales con sistemas avanzados de vigilancia masiva como el denominado Pallas o el *spyware*[215] de FinFisher, capaces de extraer información de SMS, aplicaciones de mensajería, capturas de pantallas, grabaciones audio, localizaciones de punto de acceso WiFI y SSIDs[216]. Según EFF y Lockout, este sistema obtuvo centenares de gigabytes de información de instituciones financieras, empresas, contratistas de seguridad y defensa, militares, instituciones educativas, periodistas, abogadas y defensoras de derechos humanos en más de 21 países[217]. En este sentido, Ralph Baydoun, analista digital libanés, añade que la pobre alfabetización mediática en el Líbano expone a la sociedad civil a *phishing*[218] y *spywares*[219] en sus dispositivos móviles y ordenadores[220].

---

210 **Ambri, Anas and Andrea Glioti.** "Spyware Brokers and Lebanon's Surveillance State" The New Arab. 21 de Noviembre de 2023.
Disponible en: https://www.newarab.com/investigations/spyware-brokers-and-lebanons-surveillance-state

211 Ver glosario.

212 **Bill Marczak et al.** "Mapping FinFisher's Continuing Proliferation" The Citizen Lab. 15 de Octubre de 2015.
Disponible en: https://citizenlab.ca/2015/10/mapping-finfishers-continuing-proliferation/

213 Ver glosario.

214 **Lookout and Electronic Frontier Foundation.** "Dark Caracal: Cyber-Espionage at a Global Scale." Enero de 2018.
Disponible en:
https://info.lookout.com/rs/051-ESQ-475/images/Lookout_Dark-Caracal_srr_20180118_us_v.1.0.pdf

215 Ver glosario.

216 Las siglas SSID vienen del término Service Set Identifier y en castellano significan i*dentificador del conjunto de servicio*s. Se trata del nombre que tiene una red WiFi para poder encontrarla e identificarla entre otras redes y conexiones.

217 Ibid.

218 Ver glosario.

219 Ver glosario.

220 Ralph Baydoun, entrevista personal realizada por el equipo de investigación, 6 de septiembre de 2024.

No obstante, a pesar de estos sistemas avanzados de espionaje, la arquitectura de ciberseguridad en el país es muy débil. Páginas webs gubernamentales e infraestructuras críticas son hackeadas de forma sistemática en el Líbano. Algunos ejemplos recientes fueron el hackeo de los paneles informativos del aeropuerto internacional de Beirut[221], o las páginas del Ministerio de Asuntos Sociales y del Parlamento Libanés por un grupo de hackers contratado, presuntamente, por actores israelíes[222]. Según Imad Bazzi, periodista de investigación libanés, esta situación evidencia el caos de la ciberseguridad en el país, pero también indica que no existen capacidades tan sofisticadas para el monitoreo exhaustivo de la población por parte del Gobierno[223].

En cambio, se observan otros actores no estatales nacionales e internacionales en las dinámicas de vigilancia masiva dirigida a la sociedad libanesa. Destaca el caso del *malware*[224] conocido como Flame, proveniente de Irán, para hackear móviles y ordenadores en 2012; o el uso del *malware* Zoopark, entre 2015 y 2018, con capacidad de obtener datos de mensajes SMS, navegaciones por internet, localización GPS, contraseñas, entre otros. Sin embargo, la mayor brecha de seguridad en el país ha sido el reciente ataque masivo de Israel contra militantes de Hezbollah a través de la explosión de sus dispositivos, buscas y walkie-talkies. El ataque dejó 32 muertos, incluido un niño, y miles de heridos por todo el país[225].

2. CONTROL DE LA LIBERTAD DE EXPRESIÓN EN LAS ESFERAS DIGITALES

Desde las protestas de 2019, la emergencia de medios alternativos de comunicación ha sido una tendencia creciente. Numerosas blogueras y medios digitales independientes han creado formas de comunicación más cercanas a la sociedad. Uno de los ejemplos clave fue la retransmisión en directo, con historias y testimonios a pie de calle, durante la explosión en el puerto de Beirut el 4 de agosto de 2020. Las nuevas blogueras y medios independientes utilizan redes sociales y blogs para difundir sus materiales. Para

221 **Abed Kataya.** "How Did Hackers Hijack Beirut Airport's Screens?" SMEX. 10 de enero de 2014. Disponible en: https://smex.org/how-did-hackers-hijack-beirut-airports-screens/

222 **Kataya, Abed.** "Attacks on Lebanon's Government Websites Continue: Implement Protective Standards Immediately." SMEX. 23 de enero de 2024. Disponible en: https://smex.org/attacks-on-lebanons-government-websites-continue-to-implement-protective-standards-immediately/.

223 Imad Bazzi, entrevista personal realizada por el equipo de investigación, 4 de septiembre de 2024.

224 Ver glosario.

225 **Matt Murphy and Joe Tidy.** "What We Know About the Hezbollah Device Explosions," BBC News. 20 de septiembre de 2024. Disponible en: https://www.bbc.com/news/articles/cz04m913m49o.

silenciar estas voces disidentes, el Gobierno realiza el monitoreo de los contenidos en los espacios digitales.

Desde 2006, la Oficina de Ciberdelincuencia y Derechos de Propiedad Intelectual, adjunta al Departamento de Investigaciones Criminales Especiales del ISF, es la encargada de perseguir delitos que utilizan las tecnologías de la información. Esta oficina ha sido denunciada por sus prácticas de censura y abusos sobre el ejercicio de libertad de expresión y prensa de periodistas, blogueras y otras figuras públicas del país[226]. La vigilancia y persecución de periodistas y blogueras se realiza a través de los artículos sobre difamación del Código Penal (art. 582-582, 383, 386) y la Ley de Publicaciones (art. 20-21). Según datos oficiales, la Oficina de Ciberdelincuencia investigó entre enero de 2019 y marzo de 2024, 1.684 casos de difamación[227].

En el Líbano, son una práctica habitual las detenciones, los interrogatorios e intimidaciones de defensoras de derechos humanos y periodistas[228]. Según la fundación Samir Kassir, desde 2018 se registran más de 800 abusos a periodistas como interrogatorios, coacciones, acoso por teléfono y violencia física por parte de las Fuerzas de Seguridad del Estado[229]. Algunos casos relevantes, fueron el del periodista Jean Kassir del medio digital Megaphone de 2013, detenido e interrogado por las ISF bajo una demanda de difamación por sus críticas a los líderes políticos por el caso de la explosión en el puerto de Beirut[230]. Ese mismo año, Lara Bitar del medio digital The Public Source fue convocada por la Oficina de Ciberdelincuencia por publicar un artículo sobre residuos tóxicos en Líbano[231]. Otras fuentes denuncian prácticas de coacción como amenazas de envío de *malwares*[232] para controlar la actividad de las defensoras de derechos humanos en las redes socia-

226 **Amnistía Internacional.** "Lebanon: End Use of Defamation Laws to Target Journalists and Critics." 3 de mayo de 2024. Disponible en: https://www.amnesty.org/en/latest/news/2024/05/lebanon-end-use-of-defamation-laws-to-target-journalists-and-critics/

227 Ibid.

228 **Melki, Jad, et al.** "Mapping Digital Media: Lebanon." Open Society Foundations, 15 de marzo de 2012. Disponible en: https://www.opensocietyfoundations.org/publications/mapping-digital-media-global-findings

229 **Ayyad, Safaa.** "Lebanon: Summoning Journalists in Beirut and Silencing Voices in Mount Lebanon." SMEX. 5 de abril de 2023. Disponible en: https://smex.org/lebanon-summoning-journalists-in-beirut-and-silencing-voices-in-mount-lebanon/

230 **Christou, William.** "Charges Dropped Against Lebanese Media Outlet Megaphone." The New Arab. 4 de abril de 2023. Disponible en: https://english.alaraby.co.uk/news/charges-dropped-against-lebanese-media-outlet-megaphone

231 **Safaa Ayyad.** "Lebanon: Summoning Journalists in Beirut and Silencing Voices in Mount Lebanon". 2023. Disponible en: https://smex.org/lebanon-summoning-journalists-in-beirut-and-silencing-voices-in-mount-lebanon/

232 Ver glosario.

les[233]. Access Now también informa de casos de coacción para forzar a defensoras de derechos humanos a cesar sus actividades online a través de la firma de un documento de compromiso[234].

En esta línea, Imad Bazzi apunta que la práctica común no es el monitoreo exhaustivo de las redes sociales para identificar contenidos "inapropiados". Sino más bien, un proceso donde las élites que se sienten "molestas" por el activismo político de una persona, se ponen en contacto con un partido político para activar una persecución legal a través de la fiscalía del Estado o bien poner en marcha los mecanismos de la Oficina de Ciberdelincuencia[235]. En la mayoría de los casos, estas campañas no se hacen públicas y las personas defensoras de derechos humanos simplemente desaparecen de la escena pública y/o se autocensuran[236].

La Oficina de Ciberdelincuencia cuenta con amplios recursos y tecnologías para monitorear las redes sociales y también técnicas de hackeo de móviles. En esa línea, en 2015 se identificó una propuesta de contrato entre la Oficina y la empresa Hacking Team donde se sospecha que se empleó para ciberespiar a 50 personas por 450.000 dólares[237]. En 2013, el centro Citizen Lab informó de la presencia de tecnología PacketShaper de la empresa Blue Coat para monitorear las interacciones de usuarias de las redes sociales, mensajería y comunicaciones online[238]. A partir de este monitoreo del espacio digital, el Gobierno procede al bloqueo de webs, blogs y aplicaciones. En 2015 SMEX identificó el cierre de 45 páginas web vinculadas con Israel, casas de apuestas, pornografía, prostitución, pero también de colectivos LGBTIQ+[239]. En 2018, el Ministerio de Telecomunicaciones bloqueó la plataforma para la creación del website Wix[240] y en 2020 la web para la creación de blogs

---

233 **Habib Battah.** "Who's Got Your Data?" Beirut Report. Septiembre de 2024.
Disponible en: https://beirutreport.com/whos-got-your-data-2/

234 **Access Now.** "When Cybercrime Laws Gag Free Expression: Stopping the Dangerous Trend Across MENA". 13 de enero de 2023.
Disponible en:
https://www.accessnow.org/when-cybercrime-laws-gag-free-expression-stopping-the-dangerous-trend-across-mena/

235 Imad Bazzi, entrevista personal realizada por el equipo de investigación, 4 de septiembre de 2024.

236 Ibid.

237 **SMEX.** "HackingTeam Leaks: Lebanon's Cybercrime Bureau Exploited Angry Birds to Surveil Citizens' Mobile Devices". 30 de julio de 2015.
Disponible en:
https://smex.org/hackingteam-leaks-lebanons-cybercrime-bureau-exploited-angry-birds-to-surveil-citizens-mobile-devices/

238 **Marquis-Boire et al.** "Appendix A: Summary Analysis of Blue Coat: Countries of Interest". The Citizen Lab. 15 enero de 2013. Disponible en:
https://citizenlab.ca/2013/01/appendix-a-summary-analysis-of-blue-coat-countries-of-interest/

239 **SMEX.** "Mapping Blocked Websites in Lebanon 2015". 26 de marzo de 2015.
Disponible en: https://smex.org/mapping-blocked-websites-in-lebanon-2015/

240 **Mariam S.,** "Help Us to Map Blocked Websites in 2019". SMEX. 22 de enero de 2019.
Disponible en: https://smex.org/help-us-to-map-blocked-websites-in-2019/

"Blogger" (*.blogspot.com). En una línea similar, en 2019 la aplicación de citas Grindr, fue también bloqueada sin ningún tipo de información ni justificación por parte del Ministerio de Telecomunicaciones[241]. La situación, más allá de mejorar, apunta a un endurecimiento de las penas. La nueva propuesta de Ley para Medios de Comunicación incluye penas de hasta tres años por difamar las religiones reconocidas en el país[242]. Ante esta situación, Amnistía internacional inició en 2023 una campaña para reformar las leyes sobre difamación en el Líbano bajo el hashtag #MyOpinionIsNotaCrime[243].

3. DE LA VIGILANCIA EN LAS REDES SOCIALES A LA VIOLENCIA DIGITAL

La vigilancia policial contra las personas queer se ha intensificado desde 2019. Esta persecución combina la vigilancia masiva de las esferas digitales con la identificación de personas LGBTIQ+ en las vías públicas de las principales ciudades del país. El artículo 542 del Código Penal del Líbano criminaliza las relaciones entre personas del mismo sexo[244]. Esta criminalización, se traduce en la vigilancia y el acoso online de estos colectivos. La organización británica Article 19 afirma que las aplicaciones de citas Grindr, Hornet, PlanetRomeo y Growl son utilizadas por las ISF para recoger evidencias de conductas homosexuales para arrestar y denunciar posteriormente a estas personas[245]. A este acoso online, se suma la identificación de personas LGBTIQ+ en la vía pública para confiscar y examinar sus móviles con el objetivo de encontrar imágenes e informaciones en la biblioteca de fotos o chats de WhatsApp por parte de la policía, para ser uti-

241 **SMEX.** "The Case of the Blocked Blogger: How the MoT Continues to Violate Free Expression in Lebanon". 3 de enero de 2020.
Disponible en:
https://smex.org/the-case-of-the-blocked-blogger-how-the-mot-continues-to-violate-free-expression-in-lebanon/

242 **Coalition to Defend Freedom of Expression.** "Proposed Media Law Poses Grave Threat to Freedom of Expression" Legal Agenda. 28 de noviembre de 2023.
Disponible en:
https://english.legal-agenda.com/proposed-media-law-poses-grave-threat-to-freedom-of-expression/

243 **Amnistía Internacional.** "Campaign to Decriminalize Defamation and Insult in Lebanese Laws". 8 de agosto de 2023.
Disponible en:
https://www.amnesty.org/en/latest/campaigns/2023/08/campaign-to-decriminalize-defamation-and-insult-in-lebanese-laws/.

244 **Human Rights Watch.** "Lebanon: Same-Sex Relations Not Illegal". 19 de julio de 2018.
Disponible en: https://www.hrw.org/news/2018/07/19/lebanon-same-sex-relations-not-illegal

245 **Article 19.** "Arrest and Abuse of LGBTQ+ App Users in Lebanon: A Digital Rights Crisis". 2018.
Disponible en:
https://www.article19.org/wp-content/uploads/2018/02/LGBTQ-Apps-Arrest-and-Abuse-report_22.2.18.pdf

"las elites políticas del país disponen de ejércitos electrónicos formados por miles de bots para desarrollar campañas masivas de desinformación y acoso online y así atacar la reputación de un colectivo y/o persona"

lizadas posteriormente en procesos de denuncia[246].

Las prácticas de incautaciones de móviles, ordenadores y otros medios de comunicación también se producen en campos de refugiados sirios, acentuando el aislamiento social de estas comunidades[247]. Este tipo de prácticas realizadas por las Fuerzas de Seguridad del Estado ha aumentado desde las manifestaciones de 2019. La organización SMEX indica que no hay un marco legal claro en ese sentido[248].

La criminalización y el acoso físico de colectivos LGBTIQ+ o de las personas refugiadas se justifica a través de campañas de desinformación y acoso online. Por ejemplo, desde mediados de 2024, han aumentado los discursos de odio en las redes sociales y los medios de comunicación contra las personas refugiadas sirias por parte del Gobierno libanés, líderes políticos, religiosos, e incluso de grupos afines a Hezbollah[249]. El analista digital, Ralph Baydoun detalla que las elites políticas del país disponen de ejércitos electrónicos[250] formados por miles de bots para desarrollar campañas masivas de desinformación y acoso online y así atacar la reputación de un colectivo y/o persona[251].

Los ataques reputacionales en las redes sociales se trasladan a los espacios físicos, incluyendo agresiones y asesinatos. Uno de los casos más paradigmáticos relacionado con la denuncia de casos de corrupción del Gobierno en 2019, tuvo graves implicaciones laborales y para la integridad física y psicológica (así como también en la de sus familiares) de la periodista implicada[252]. Se realizaron campañas de violencia digital y lawfare, incitación al odio y doxxing[253]. El caso también derivo en una sentencia judicial de un año de prisión

246 **Article 19.** "Digital Crime Scenes: How Counterterrorism Laws Undermine Free Expression". Marzo de 2022. Disponible en: https://www.article19.org/wp-content/uploads/2022/03/Digital-Crime-Scenes-Report-3.pdf

247 **ACHR.** "Lebanon: Censorship and Violations of Free Speech". Arab Center for Human Rights. 13 de enero de 2023. Disponible en: https://www.achrights.org/en/2023/01/13/12910/

248 **Marianne Rahme.** "Device Seizures in Lebanon: A Report on the Violations of Digital Rights". SMEX. 2021. Disponible en: https://smex.org/wp-content/uploads/2021/02/SMEX-Device-Seizures-Report-2021-eng.pdf

249 **Salhani, Justin.** "Targeted: How Misinformation Puts Lebanon's Syrian Refugees in Danger" The Tahrir Institute for Middle East Policy (TIMEP). 28 de agosto de 2024.
Disponible en:
https://timep.org/2024/08/28/targeted-how-misinformation-puts-lebanons-syrian-refugees-in-danger/

250 Ver glosario.

251 Ralph Baydoun, entrevista personal realizada por el equipo de investigación, 6 de septiembre de 2024.

252 Por razones de seguridad para la persona defensora, se omite el nombre y las referencias del caso.

253 Ver glosario.

para esta mujer defensora por una causa de difamación tras denunciar públicamente la violencia contra defensoras de derechos humanos ejercida por parte de miembros del partido cristiano Free Patriotic Movement. Las mujeres son especialmente afectadas por la violencia digital. Según SMEX, entre 2020 y 2023, el 80% de los objetivos de violencia digital en el Líbano eran mujeres[254].

254 **Ayyad, Safaa**. "80% of Women in Lebanon Face Digital Violence" SMEX. 4 de marzo de 2024. Disponible en: https://smex.org/80-of-women-in-lebanon-face-digital-violence/

VI

LA GUERRA DE SIRIA EXACERBA LA VIGILANCIA MASIVA

El ciberespacio en Siria está fuertemente regulado y controlado por el Gobierno a través de varios ministerios y entidades, de forma más intensa a partir de los acontecimientos que tuvieron lugar durante la Primavera Árabe. El aparato securitario del Gobierno sirio está compuesto por la inteligencia militar siria, en la que diferentes unidades colaboran para ejercer control y vigilancia cibernética sobre la población. En este sentido, la Unidad 225 es responsable de monitorear las comunicaciones internas[255]. Esta unidad tiene entre otros, la capacidad de bloquear números específicos, terminar llamadas, deshabilitar servicios de SMS[256]. Se encuentra también la Unidad 211[257], conocida como la rama "técnica" o "informática", que se centra en la regulación del acceso a sitios web, gestionando las comunicaciones inalámbricas y proporcionando apoyo técnico a la Unidad 225. Finalmente, la Unidad 237[258] se especializa en el seguimiento e intervención de llamadas inalámbricas.

"El ciberespacio en Siria está fuertemente regulado y controlado por el gobierno a través de varios ministerios y entidades, de forma más intensa a partir de los acontecimientos que tuvieron lugar durante la Primavera Árabe"

Cuando se iniciaron las protestas generalizadas en la región Maghreb y Mashreq, especialmente en Egipto y Túnez, el presidente sirio Assad dedujo que las protestas habían logrado derrocar a sus líderes porque los Gobiernos no reprimieron las manifestaciones con suficiente antelación. El Gobierno de Assad ya era conocido antes de la guerra por censurar el contenido de Internet en el país[259]. Tan pronto como comenzaron las protestas, el presidente sirio Assad expulsó del país a las periodistas extranjeras para controlar la cobertura periodística de los acontecimientos y el uso que estos hacían

255 **Gsell, Eveline, and Maik Maurer.** "State-sponsored Cyber Operations in the Middle East: Proxies and Cyber Sovereignty in the GCC and Beyond." Center for Security Studies (CSS), ETH Zurich. Mayo de 2017. Disponible en: https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2017-05.pdf.

256 **Helwani, I.** "Cyberactivism in Syria." 2024. Disponible en: https://dergipark.org.tr/en/download/article-file/3842663.

257 **Syrian Network for Human Rights.** "Syrian Security Branches and Persons in Charge." Disponible en: https://snhr.org/public_html/wp-content/pdf/english/Syrian_security_branches_and_Persons_in_charge_en.pdf

258 **Syrian Network for Human Rights.** "Syrian Security Branches and Persons in Charge." Disponible en: https://snhr.org/public_html/wp-content/pdf/english/Syrian_security_branches_and_Persons_in_charge_en.pdf

259 **Tkacheva, O., Schwartz, L. H., Libicki, M. C., Taylor, J. E., Martini, J., & Baxter, C.** *Internet Freedom and Political Space*. 2013. RAND Corporation. Disponible en: https://www.jstor.org/stable/10.7249/j.ctt4cgd90

de internet[260]. Los diferentes proveedores de Internet en Siria operan bajo la empresa Syrian Telecom (STE), propiedad del Gobierno. El STE, establecido en 1975, es fundamental en el dominio cibernético de Siria, proporcionando conectividad global y regulando el flujo de información. Asimismo, en numerosas ocasiones, el Gobierno sirio bloqueó internet y la telefonía móvil durante varios días para impedir, entre otras, que las manifestantes publicaran vídeos, imágenes o comentarios sobre los acontecimientos en las redes sociales[261].

"Bajo el pretexto de combatir la ciberdelincuencia, en abril de 2022 se introduce la nueva Ley de Ciberseguridad Siria, que se ha convertido en parte de las tácticas legales represivas impuestas por el régimen sirio para criminalizar la libertad de expresión y el libre flujo de información"

Una década después de que Assad reprimiera las manifestaciones de la población siria, el régimen continúa consolidando su poder criminalizando la libertad de expresión y reduciendo los espacios cívicos para reprimir cualquier forma de disidencia u oposición. En este marco de vulneraciones sistemáticas de derechos es donde se introdujo en abril de 2022 la nueva Ley de Ciberseguridad Siria[262], que se ha convertido de *facto* en parte de las tácticas legales represivas impuestas por el régimen sirio para criminalizar la libertad de expresión y el libre flujo de información con el pretexto de combatir la ciberdelincuencia.

260 **Hossain, M.** The impact of cyber capabilities in the Syrian civil war. 2020. Small Wars Journal. 2016. Disponible en: https://smallwarsjournal.com/jrnl/art/the-impact-of-cyber-capabilities-in-the-syrian-civil-war

261 **Khazan, O.** "Syria Internet outage: How it might have happened and what it means." The Washington Post, 30 noviembre 2012. Disponible en: https://www.washingtonpost.com/news/worldviews/wp/2012/11/30/syria-internet-outage-how-it-happened/

262 **Index on Censorship.** "Syria Passes Draconian Cybersecurity Law." 2022. Disponible en: https://www.indexoncensorship.org/2022/05/syria-passes-draconian-cybercrime-laws/

1. LA REPRESIÓN DE LAS DISIDENCIAS POLÍTICAS A TRAVÉS DE LOS EJÉRCITOS ELECTRÓNICOS[263]

La libertad de expresión está sujeta a un estricto control en toda Siria. El régimen ha incrementado recientemente su ya estricta legislación con la aprobación en abril de 2022, de un nuevo Decreto-Ley sobre Ciberdelincuencia[264], que impone duras penas para cualquier actividad en línea que socave el "prestigio del Estado" o la "unidad nacional", entre otras disposiciones vagas. Uno de los puntos clave de esta nueva Ley es el control que pretende aplicar sobre lo que describe como *"fake news"*[265] que puedan llegar a socavar el prestigio del Estado o perjudicar la unidad nacional. Este delito lleva aparejado una pena privativa de libertad de hasta 5 años y sanciones económicas cuantiosas. Según el Syrian Network for Human Rights (SNHR), las consecuencias de la entrada en vigor de esta Ley en el marco jurídico sirio han sido nefastas para la población civil, especialmente para colectivos de activistas, defensoras de derechos humanos y opositoras al régimen. Al menos una persona ha muerto a consecuencia de tortura y 146 personas han sido arrestadas arbitrariamente bajo el nuevo marco legal[266].

"Según un informe del SNHR, la Ley para establecer un Ministerio de Medios de Comunicación es un instrumento para consolidar el control del régimen sobre el contenido de los medios de comunicación, imponer más censura contra la prensa y las publicaciones, así como para imponer más restricciones a la producción televisiva"

La SNHR, publicó el pasado junio de 2024 un informe en el que analizaba otra ley más reciente sobre el establecimiento de un Ministerio de Medios de Comunicación[267]. Según el SNHR esta Ley es un instrumento para consolidar el control del régimen sobre el conte-

263 Ver glosario.

264 **Tahrir Institute for Middle East Policy.** "Understanding Assad's New Cyber Crackdown." 2022. Disponible en: https://timep.org/2022/10/05/understanding-assads-new-cyber-crackdown-in-syria/

265 Ver glosario.

266 **Syrian Network for Human Rights.** "Report." 2022. Disponible en: https://snhr.org/wp-content/uploads/2023/08/R230812E.pdf

267 **SNHR.** "The 19/2024 Law. 2024." Disponible en: https://snhr.org/blog/2024/06/13/the-syrian-regimes-law-no-19-of-2024-on-establishing-a-media-ministry-blatantly-violates-freedom-of-media-opinion-and-expression/

nido de los medios de comunicación, imponer más censura contra la prensa privada y las publicaciones que ingresan al país, e imponer más restricciones a la producción televisiva. En este sentido, entre marzo de 2011 y mayo de 2024, SNHR documentó el asesinato de 717 periodistas[268].

Con anterioridad a la promulgación de esta Ley, ha habido diversos grupos de hackers que han dado apoyo digital al régimen de Assad a lo largo del conflicto. En este sentido, en 2016, se publicó una investigación sobre Group 5[269], un colectivo de hackers proiraní que daba apoyo al régimen de Assad. El grupo de hackers estableció páginas web con nombres como *AssadCrimes* como parte de sus elaborados esquemas de ingeniería informática para hacer caer en la trampa a miembros de la oposición y defensoras de derechos humanos que, al clicar en el enlace, habilitaban el acceso a toda la información de sus dispositivos.

Otro grupo de hackers que ha dado apoyo a Assad es el Syrian Electronic Army (SEA)[270]. El SEA opera con el apoyo del régimen, y utiliza ataques DDoS[271], estafas de *phishing*[272] y otros trucos para vigilar a defensoras de derechos humanos y opositoras al régimen, así como a los medios de comunicación críticos. Una investigación en 2013 demostró que el nombre de dominio del sitio web del grupo fue registrado en mayo de 2011 por la Sociedad de Computación Siria (SCS), una organización que fue dirigida por el presidente sirio Bashar al-Assad en 1995 antes de que asumiera la presidencia[273]. Dentro de este grupo habría un subgrupo llamado *The Syrian Malware Team* (SMT) que utilizó tecnología RAT (*Remote Access Tool*) para penetrar los dispositivos móviles y acceder a toda su información[274]. Aun así, no está claro si los miembros de estos grupos tienen un vínculo directo con el Gobierno sirio o simplemente son un grupo de hackers informáticos pro-Assad.

268 **SNHR**. "World Press Freedom Day." 2024
Disponible en: https://snhr.org/wp-content/uploads/2024/05/S240419E.pdf

269 **The Citizen Lab**. "Group 5, Syria and the Iranian connection." 2016.
Disponible en: https://citizenlab.ca/2016/08/group5-syria/

270 **González, R.** "Syria's Digital Counter-Revolutionaries." *The Atlantic*, 2011.
Disponible en:
https://www.theatlantic.com/international/archive/2011/08/syrias-digital-counter-revolutionaries/244382/

271 Ver glosario.

272 Ver glosario.

273 **Open Net Initiative.** "Syrian Electronic Army: Disruptive Attacks and Hyped Targets."
Disponible en: https://opennet.net/syrian-electronic-army-disruptive-attacks-and-hyped-targets.

274 **Prince, B.** Syrian Malware Team uses Blackworm RAT in attacks. *Security Week*. 1 septiembre 2014.
Disponible en: https://www.securityweek.com/syrian-malware-team-uses-blackworm-rat-attacks/

2. CENSURA Y CONTROL DE LAS TELECOMUNICACIONES EN EL ESPACIO DIGITAL

El Gobierno sirio puso en marcha su primer sistema de monitoreo de redes a nivel nacional en 1999. El sistema, encargado por la empresa Syrian Telecom Siria (STE), fue diseñado para monitorear la telefonía móvil, fija e Internet. Actualmente los ataques cibernéticos son comunes y el control de Internet se utiliza como arma de guerra: son frecuentes los apagones intencionados, utilizados para desactivar temporalmente las redes de comunicación establecidas por grupos contrarios al régimen. Inmediatamente después del levantamiento de 2011, el régimen sirio cerró todo acceso a Internet en el este de Siria y sucedieron apagones intermitentes que han continuado durante todo el conflicto además de restringir por completo contenido en páginas web que cubrían temas que el régimen consideraba sensibles[275].

"Los ataques cibernéticos y el control de Internet son comunes y se utilizan como armas de guerra. Los apagones intencionados son utilizados para desactivar las redes de comunicación de grupos contrarios al régimen"

Unos años antes de las revueltas árabes, el Gobierno sirio construyó sistemas de monitoreo de comunicaciones a través de diversos proyectos en los cuales el conocimiento y experiencia de empresas del norte global fue básico. En este sentido, empresas como VASTech (Sudáfrica) y AGT (Emiratos Árabes Unidos – Alemania) contribuyeron en gran medida al estado represivo de vigilancia de Siria ofreciendo soluciones de control, vigilancia y censura de las redes[276]. Durante el inicio del conflicto sirio, el Gobierno utilizó dispositivos de monitoreo de telecomunicaciones de Blue Coat Systems, una empresa con sede en Estados Unidos, para el filtrado de redes, la censura y la vigilancia. A pesar de las sanciones de Estados Unidos que prohíben las ventas a Siria, estos dispositivos se enviaron a un distribuidor en Dubai y fueron posteriormente remitidos a Siria[277].

Otras empresas occidentales establecieron vínculos con el régimen de Assad al distri-

275 **Le VPN.** "Internet Censorship in Syria."
Disponible en: https://www.le-vpn.com/internet-censorship-syria/

276 **Privacy International**. "Building Syria's Surveillance State." 2016.
Disponible en: https://privacyinternational.org/sites/default/files/2017-12/OpenSeason_0.pdf

277 **The Citizen Lab.** "Behind Blue Coat." 2011.
Disponible en: https://citizenlab.ca/2011/11/behind-blue-coat/

buir tecnología de vigilancia digital. Una de estas empresas es la italiana Area SpA[278], que vende sistemas de monitoreo capaces de capturar el tráfico de Internet, interceptar conversaciones y rastrear objetivos a través de GPS y que obtuvo un contrato gubernamental en Siria y en Egipto[279]. La compañía italiana habría comenzado a instalar sistemas de monitoreo de redes que darían al Gobierno sirio la capacidad de interceptar, escanear y catalogar prácticamente todos los correos electrónicos que fluyen a través del país, así como el rastreo de objetivos y el mapeo de las redes de contactos electrónicos de la población siria[280].

Una de las empresas que también facilitó la implementación de una estructura de vigilancia digital en Siria es la compañía alemana Utimaco[281]. Según información del European Center for Constitutional and Human Rights (ECCHR), Utimaco participó juntamente con Area SpA de un sistema de vigilancia administrado por Syrian Telecom[282]. ECCHR presentó en enero de 2018 una denuncia penal ante la Fiscalía Federal Alemana donde aparecía la empresa por su supuesta complicidad en crímenes de lesa humanidad y crímenes de guerra. La compañía francesa Qosmos también fue denunciada ante un Tribunal francés por organizaciones de la sociedad civil que la acusaron de suministrar al Gobierno sirio el software de inspección profunda de paquetes (DPI)[283] que permitió al régimen rastrear a defensoras de derechos humanos[284], disidentes y miembros de la oposición algunos de los cuales acabaron siendo torturados o ejecutados después de que comenzara el levantamiento inicial contra el régimen en 2011[285].

---

278 **Privacy International.** "Building Syria's Surveillance State." 2016.
Disponible en: https://privacyinternational.org/sites/default/files/2017-12/OpenSeason_0.pdf

279 **Vice. "**La policía italiana allana la sede de la empresa SpA." 2016.
Disponible en:
https://www.vice.com/en/article/italian-cops-raid-surveillance-tech-company-area-spa-selling-spy-gear-to-syria/

280 **Electronic Fronteir Foundation (EFF).** "Spy-tech companies and their authoritarian costumers. 2012."
Disponible en:
https://www.eff.org/deeplinks/2012/02/spy-tech-companies-their-authoritarian-customers-part-ii-trovicor-and-area-spa

281 **Der Spiegel.** "Is Syrian monitoring protesters with German technology?" 2011.
Disponible en:
https://www.spiegel.de/international/world/police-state-is-syria-monitoring-protesters-with-german-technology-a-796510.html

282 **European Center for Constitutional Rights.** Surveillance in Syria.
Disponible en:
https://www.ecchr.eu/en/case/surveillance-in-syria-european-firms-may-be-aiding-and-abetting-crimes-against-humanity/

283 Ver glosario.

284 **Corpwatch.** "French Tribunal investigates Qosmos." 2015.
Disponible en:
https://www.corpwatch.org/article/french-tribunal-investigates-qosmos-over-surveillance-software-use-syria

285 **Federación Internacional por los Derechos humanos.** "Qosmos, objeto de una investigacion judicial." 2014.
Disponible en:
https://www.fidh.org/es/region/europa-y-asia-central/francia/15435-francia-qosmos-objeto-de-una-investigacion-judicial-por-complicidad-en

En este sentido, miembros de la sociedad civil siria conocen perfectamente que sus comunicaciones están siendo vigiladas y toman medidas al respecto. Según comparte Abdulaziz Ramadan[286], director ejecutivo de DOZ e.V.[287] "acordamos determinados niveles de seguridad en como compartir la información en plataformas como WhatsApp". "Tenemos que pensar en nuevas herramientas que nos permitan no sentirnos amenazados y ejercer libremente nuestro derecho fundamental a la libertad de expresión".

3. VIGILANCIA MASIVA Y CONTROL DEL ACTIVISMO EN LA DIÁSPORA: EL ROL DE LAS MISIONES DIPLOMÁTICAS

Después de la represión sistemática durante la Primavera Árabe y aún más si cabe durante la guerra siria, miles de defensoras de derechos humanos huyeron del país. Sin embargo, el régimen sirio continuó la persecución más allá de sus fronteras[288]. Una investigación realizada por el Centro de Justicia y Rendición de Cuentas de Siria (SJAC, por sus siglas en inglés) reveló documentos que prueban que la vigilancia en el extranjero sobre la sociedad civil siria se llevó a cabo sistemáticamente en toda la red de misiones diplomáticas del régimen[289]. Entre 2013 y 2015, SJAC obtuvo acceso a aproximadamente 483.000 páginas de documentos clasificados de instalaciones estatales sirias abandonadas. Gracias a esta documentación, SJAC descubrió que la vigilancia sobre la sociedad civil siria se daba en lugares tan dispares como España, Bielorrusia, Bélgica, Chipre, Egipto, Francia, Grecia, Irak, Japón, Jordania, Líbano, Rusia, Arabia Saudí, Turquía, Ucrania, Reino Unido y Yemen. Estos documentos fueron emitidos entre 2009 y 2012 por varias agencias de

"Según el Centro de Justicia y Rendición de Cuentas de Siria, la sociedad civil siria en el extranjero ha sido vigilada sistemáticamente por el régimen"

286 Abdulaziz Ramadan, entrevista realizada en el marco de The Nonviolence Factory, noviembre de 2023. Equipo NOVACT, SUDS, IRIDIA y ODHE.

287 Organización de la sociedad civil siria con sede en Alemania.

288 **Amnistia Internacional.** "La larga mano de la Mukhabaraat." 2021.
Disponible en: https://www.amnesty.org/es/wp-content/uploads/sites/4/2021/07/mde240572011es.pdf

289 **SJAC.** "Walls have ears". 2022.
Disponible en: https://syriaaccountability.org/content/files/2022/04/Walls-Have-Ears-English.pdf

inteligencia dependientes del Ministerio del Interior y el Ministerio de Defensa. Estas prácticas de vigilancia y control de la sociedad civil siria se han dado también en el Estado español, donde grupos de opositores al régimen sirio protestaron ante la embajada de Siria en Madrid en determinadas ocasiones.

Según la información obtenida por Amnistía Internacional[290], el mismo personal de la embajada donde se dieron las protestas fotografiaba y grababa en video para identificar a las participantes. Este material era enviado posteriormente al *Mukhabarat*[291] (servicio de inteligencia sirio) y desde allí se identificaba a cada una de las personas participantes y se tomaba medidas contra ellas y sus familiares. Algunas de las consecuencias a las que se enfrentaban las personas que participaban de estas protestas era la obstaculización de procedimientos administrativos que debían llevar a cabo en la embajada[292]. Al mismo tiempo, estas prácticas legítimas de protesta se convierten en la excusa perfecta del régimen sirio para amedrentar, amenazar, arrestar e incluso golpear a familiares y seres queridos que la comunidad opositora siria en el extranjero aún tiene en el país[293].

290 **Amnistía Internacional.** "Syria: The long reach of the Mukhabaraat: Violence and harassment against Syrians abroad and their relatives back home." 2021.
Disponible en: https://www.amnesty.org/en/documents/mde24/057/2011/en/

291 Mukhabarat, que en árabe significa inteligencia, es un término general para las agencias de inteligencia, en el caso sirio, Inteligencia General (también conocida como Seguridad del Estado), Inteligencia Militar, Inteligencia de la Fuerza Aérea y Seguridad Política. **Amnistía Internacional.** "Syria: The long reach of the Mukhabaraat: Violence and harassment against Syrians abroad and their relatives back home." Índice MDE 24/057/2011. 3 de octubre de 2011.
Disponible en: https://www.amnesty.org/en/documents/mde24/057/2011/en/.

292 **Amnistía Internacional.** "Syria: The long reach of the Mukhabaraat: Violence and harassment against Syrians abroad and their relatives back home." Índice MDE 24/057/2011, 3 de octubre de 2011.
Disponible en: https://www.amnesty.org/en/documents/mde24/057/2011/en/.

293 **Amnistía Internacional.** "Syria: The long reach of the Mukhabaraat: Violence and harassment against Syrians abroad and their relatives back home." 2011.
Disponible en: https://www.amnesty.org/en/documents/mde24/057/2011/en/

4. CONTROL SOBRE LA COMUNIDAD KURDA EN EL NORESTE DE SIRIA

En 2022 el SJAC publicó un informe[294], después de analizar documentación sensible abandonada por el Gobierno Sirio, que evidencia la persecución contra la población kurda. SJAC identificó un total de 349 páginas que mencionaban a personas o actividades kurdas, lo que se refleja en prácticas represivas sistemáticas que atentan contra los derechos humanos. Algunas de las medidas que se han utilizado para la persecución de la comunidad kurda y que se han descubierto gracias a la investigación de SJAC son[295]:

- Violación de la libertad de reunión y de expresión: Varias páginas invitaban al aparato de seguridad sirio a interrumpir directamente las protestas planificadas y a requerir mayores permisos específicamente para que los grupos kurdos se reunieran públicamente;

- Violación de los derechos culturales: Dos de las páginas analizadas transmitían el temor de que la expresión de la cultura y el idioma kurdos amenazaran la unidad siria. En respuesta al aumento de las actividades políticas kurdas, una página describía el plan del Gobierno para criminalizar todas las actividades «nacionalistas» kurdas;

- Supervisión de la propiedad y la economía kurda: Los documentos también indicaban el temor del acceso kurdo a la tierra y la riqueza. Algunas páginas recomendaban que los municipios exigieran permisos antes de que compraran o vendieran tierras, que se vigilaran de cerca los patrones de compra de la comunidad kurda y que se castigara a esta por participar en transacciones inmobiliarias no autorizadas;

- Diluir la composición étnica en las zonas kurdas: Una página invitaba a las fuerzas estatales sirias a que se presionara a las tribus árabes para que se trasladaran a la provincia de Hassakeh, aparentemente para diluir la mayoría kurda y al mismo tiempo otra página recomendaba específicamente evitar que el kurdo sea el grupo étnico mayoritario en cualquier región;

- Persuasión e intimidación de líderes kurdas: Los documentos ordenaban específicamente que líderes kurdas fueran cooptadas y que se tomaran medidas para alentar a las personas kurdas a identificarse más como sirias a través de métodos de persuasión e intimidación para atraer y amenazar a las líderes kurdas para que se alinearan con el Gobierno.

294 **SJAC.** "Walls Have Ears." 2022.
Disponible en: https://syriaaccountability.org/content/files/2022/04/Walls-Have-Ears-English.pdf.

295 Ibid.

“Desde el año 2019 hay constancia de campañas de espionaje digital hacia la comunidad kurda. Perfiles falsos en Facebook invitaban a descargar una app infectada con un virus troyano que podía acceder a registros de llamadas, ficheros y/o tomar fotografías”

Además, desde al menos el año 2019 ha habido en las redes diversas campañas de espionaje digital dirigidas contra la comunidad kurda. En este sentido, la empresa de ciberseguridad ESET y el centro de inteligencia chino QiAnXin Threat Intelligence Center descubrieron en 2020[296] que a través de perfiles falsos de Facebook que invitaban a descargar aplicaciones de Android[297], se activaba un virus troyano de acceso remoto[298] que permitía acceder al registro de llamadas, consultar y exportar ficheros y tomar fotografías, entre otras funciones.

296 **Stone, J.** “Spyware APP Designed to Monitor Kurdish.” CyberScoop. 8 de septiembre de 2021. Disponible en: https://cyberscoop.com/spyware-kurds-eset-bladehawk-iran/.

297 **Report Blade Eagle Organization.** "Qianxin Intelligence Center." 2020. Disponible en: https://ti.qianxin.com/blog/articles/Blade-hawk-The-activities-of-targeted-the-Middle-East-and-West-Asia-are-exposed/

298 Ver glosario.

VII

TESTED IN SURVEILLANCE: PALESTINA COMO CAMPO DE PRUEBAS DEL ESTADO DE ISRAEL

La vigilancia militar israelí sobre el pueblo palestino tiene una larga historia que se remonta a la fundación del Estado de Israel en tierra palestina en 1948, cuando 750.000 personas palestinas fueron expulsadas de sus hogares e Israel sometió a las que se quedaron a un gobierno militar marcado por una vigilancia generalizada[299]. Es en este marco de vulneraciones sistemáticas, donde las empresas de ciberseguridad forman parte de una red de vigilancia cada vez más grande que está afianzando el control del Gobierno de Israel sobre la población palestina, y que ayuda a mantener el sistema de *apartheid* israelí[300].

"La libertad de desarrollar y testear todo tipo de tecnología armamentística y de seguridad sobre la población palestina ha permitido a que Israel emergiera como líder mundial en tecnología de vigilancia a principios del siglo XXI, tendencia que se ha mantenido en el tiempo y a la cual el genocidio actual en Gaza parece no afectar"

La libertad de desarrollar y testear todo tipo de tecnología armamentística y de seguridad sobre la población palestina ha permitido a que Israel emergiera como líder mundial en tecnología de vigilancia a principios del siglo XXI, tendencia que se ha mantenido en el tiempo y a la cual el genocidio actual en Gaza parece no afectar[301]. En este sentido, el ejército de Israel (IDF por sus siglas en inglés) es la principal incubadora de *startups* de ciberseguridad del mundo. El servicio militar en general y concretamente la Unidad de inteligencia y ciberseguridad 8200 del ejército israelí, sirven como auténticas experiencias profesionales para los jóvenes militares antes de incorporarse al sector privado de la ciberseguridad[302]. No sorprende entonces que un estudio de 2018 citado por el diario israelí *Haaretz* estimara que el 80% de las 2.300 personas que fundaron las 700 empresas de ciberseguridad de Israel habían pasado por esta Unidad de Inteligencia del ejército israelí[303].

Ya durante las revueltas árabes, plataformas como Facebook, Instagram y TikTok fueron parte integral de las protestas generalizadas en toda la región Mashreq, incluida Palestina. En este sentido el Estado de Israel implementó un férreo control de las redes sociales, volviéndose un elemento clave en la vigilancia y la posterior represión de la población

299 **Institute for Middle East Understanding.** "Quick facts: Palestinian Refugees" 19 de junio de 2024. Disponible en: https://imeu.org/article/quick-facts-palestinian-refugees

300 **Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos (OHCHR)**. "Israel's 55-year occupation of Palestinian Territory is apartheid: UN Human Rights Expert." 22 de marzo de 2022. Disponible en: https://www.ohchr.org/en/press-releases/2022/03/israels-55-year-occupation-palestinian-territory-apartheid-un-human-rights.

301 **Nachmani, O**. "Over 2.5B$ in Acquisitions: Israel Still a Cyber Leader." 2024. Disponible en: https://iamondemand.com/blog/over-2-5b-in-acquisitions-israel-still-a-cyber-leader/.

302 **Daza, F.** "Los muros Invisibles de la Ocupación". Novact. 2023. Disponible en: https://novact.org/wp-content/uploads/2023/10/Informe_Muros-invisibles_ocupacion.pdf.

303 **Transnational Institute.** "Israel: Modelo de Estado Coercitivo." 13 de julio de 2021. Disponible en: https://www.tni.org/es/art%C3%ADculo/israel-modelo-de-estado-coercitivo.

palestina[304]. Más tarde, en el marco del COVID-19 Israel implantó una serie de medidas legales que justificaban la expansión de los sistemas de vigilancia y de las tecnologías de control[305]. En este sentido, la pandemia del COVID-19 contribuyó a normalizar y legitimar los abusos de poder y las violaciones de derechos humanos cometidos por las fuerzas de seguridad del Estado de Israel en connivencia con las empresas de ciberseguridad que desarrollan e implementan estas tecnologías[306]. Una de estas empresas es NSO Group, que en marzo de 2020 lanzó un software de rastreo de contactos llamado Fleming[307]. Más recientemente y meses antes de la invasión de Gaza, el Estado de Israel aprobó una ley conocida por la oposición como "Big Brother in Public Spaces" con la cual se promueve y regula el uso de sistemas biométricos en el espacio público, incluso por parte de la policía de Israel. El proyecto de ley incluye implicaciones de gran alcance en relación con el derecho a la privacidad. El sistema que se pretende implementar permitiría el procesamiento de fotografías de personas para compararlas en una base de datos[308] [309].

1. GENOCIDIO Y USO DE HERRAMIENTAS DE INTELIGENCIA ARTIFICIAL

Israel mantiene un bloqueo a la Franja de Gaza por tierra, mar y aire desde hace 17 años. En octubre de 2023 Israel inició una nueva invasión del territorio dando comienzo al genocidio actual sobre la población palestina. Paralelamente, el ejército de Israel y colonos armados han lanzado una campaña de ataques sistemáticos contra la población de Cisjordania. Estos ataques han propiciado una escalada en las prácticas de control y vigilan-

304 **7amleh.** "Israel's Surveillance Industry and Human Rights." Diciembre 2023.
Disponible en: https://7amleh.org/storage/Israel%E2%80%99s%20Surveillance%20Industry%20english4.pdf

305 **Nature.** "Mass Surveillance technologies to fight coronavirus spread: the case of Israel." 26 de mayo de 2020.
Disponible en:
https://www.researchgate.net/publication/341646871_Mass-surveillance_technologies_to_fight_coronavirus_spread_the_case_of_Israel

306 **Spilka, Dmytro.** "Israeli Cyber Security Stocks Are Set to Outperform in the Age of Remote Work." The Times of Israel, 22 de diciembre de 2020.
Disponible en:
https://blogs.timesofisrael.com/israeli-cyber-security-stocks-are-set-to-outperform-in-the-age-of-remote-work/.

307 **Forensic Architecture.** "NSO's Group breach of private data with "Fleming"." 30 de diciembre de 2020.
Disponible en:
https://forensic-architecture.org/investigation/nso-groups-breach-of-private-data-with-fleming-a-COVID-19-contact-tracing-software

308 **Ley de Vigilancia del Espacio Público de Israel**.
Disponible en: https://www.law.co.il/media/computer-law/police_ordinance_amendment_bill2023.pdf

309 **Katz, Yaakov.** "Israel to Allow Police Use of Facial Recognition Cameras in Public Areas." *The Jerusalem Post.* 20 de diciembre de 2023.
Disponible en: https://www.jpost.com/israel-news/politics-and-diplomacy/article-731906.

cia sobre la población palestina. Lo novedoso de esta nueva ola de violencia y represión de la población palestina es el uso de herramientas de inteligencia artificial (IA).

"Lo novedoso de esta nueva ola de violencia y represión de la población palestina es el uso de herramientas de inteligencia artificial (IA)"

En este sentido, el ejército israelí ha desarrollado un programa basado en inteligencia artificial[310] conocido como «Lavender» y "Gospel[311]." Según oficiales de las unidades de inteligencia israelíes, que han participado de primera mano en el uso de la IA en Gaza, Lavender ha desempeñado un papel central en el bombardeo de población civil palestina, especialmente durante las primeras etapas de la guerra[312]. A la utilización de estos sistemas automatizados de generación de objetivos humanos y objetivos de infraestructura como Lavender y Gospel respectivamente, se les une otra herramienta llamada *"¿Where is Daddy?"*, un sistema de inteligencia artificial diseñado para rastrear y seleccionar a presuntos militantes de Hamás cuando están en casa con sus familias[313].

Otro tipo de herramientas de IA que han sido utilizadas en los ataques contra la Franja de Gaza son los sistemas de armas autónomas letales (LAWS por sus siglas en inglés) y armas semi autónomas (semi-LAWS)[314]. El ejército israelí ha sido pionero en el uso de cuadricópteros a control remoto equipados con ametralladoras y misiles para vigilar, controlar y atacar a personas e infraestructuras[315]. Israel ha sido clasificado como el principal proveedor de drones suicidas del mundo[316]. Ambas tecnologías han sido desarrolladas por Israel Aerospace Industries (IAI)[317].

---

310 **Yuval, A.** "Lavender, The AI machine directing Israel's bomibing in Gaza." *+972 Magazine*. 3 de abril de 2024. Disponible en: https://www.972mag.com/lavender-ai-israeli-army-gaza/

311 **Yuval, A.** "A mass assassination factory." *+972 Magazine*. 30 de noviembre de 2023. Disponible en:https://www.972mag.com/mass-assassination-factory-israel-calculated-bombing-gaza/

312 **Frankel Pratt, S**. "When AI decides who lives and dies." *Foreign Policy*. 2 de mayo de 2024. Disponible en: https://foreignpolicy.com/2024/05/02/israel-military-artificial-intelligence-targeting-hamas-gaza-deaths-lavender/

313 **Democracy Now! "**Israel's AI Surveillance System for Palestinians." 5 de abril de 2024. Disponible en: https://www.democracynow.org/2024/4/5/israel_ai.

314 **Access Now.** "Artificial Genocidal Intelligence." 2024. Disponible en: https://www.accessnow.org/publication/artificial-genocidal-intelligence-israel-gaza/

315 **Technology and Innovation.** "The future of defending Israel, Jaguar". 27 de abril de 2021. Disponible en: https://www.idf.il/en/mini-sites/technology-and-innovation/jaguar-the-idf-s-newest-most-advanced-robot/

316 **Globes.** "Israel Ranked as World's Top Supplier of Suicide Drones." 5 de octubre de 2023. Disponible en: https://en.globes.co.il/en/article-israel-ranked-as-worlds-top-supplier-of-suicide-drones-1001489297.

317 **The Jerusalem Post.** "IAI Exhibits Upgraded HAROP Suicide Drone for Clients." 15 de junio de 2016. Disponible en: https://www.jpost.com/Israel-News/IAI-exhibits-upgraded-HAROP-suicide-drone-for-clients-405266.

Una de las empresas involucradas en el actual genocidio de Gaza es el mayor fabricante de armas de Israel, Elbit Systems, principal proveedor del ejército israelí. Actualmente el 85% de todas las armas, sistemas de vigilancia y herramientas que utiliza el ejército israelí han sido fabricadas por Elbit, incluidos los drones militares Skylark y Hermes, que forman la mayoría de la flota de grandes aviones no tripulados de Israel y que se han utilizado ampliamente en Gaza[318]. El uso de este tipo de herramientas tiene en muchos casos como consecuencia, la muerte de civiles y plantean cuestiones relativas a las violaciones del Derecho Internacional Humanitario (DIH), entre ellas, *el principio de distinción* donde se debe cumplir el requisito de distinguir estrictamente entre objetivos civiles y militares[319].

"La creciente oleada violenta en Cisjordania y Jerusalén Este y el genocidio en Gaza han propiciado la aparición de una nueva tendencia de defensa civil y de resistencia a la ocupación. Periodistas, blogueras, creadoras de contenido e influencers palestinas muestran el día a día de las violaciones de derechos humanos llevadas a cabo por Israel en Gaza y en la Cisjordania ocupada, mientras ven peligrar su trabajo y su vida"

La creciente oleada violenta en Cisjordania y Jerusalén Este y el genocidio en Gaza ha propiciado la aparición de una nueva tendencia de defensa civil y de resistencia a la ocupación [320]. Periodistas, blogueras, creadoras de contenido e influencers palestinas muestran el día a día de las violaciones de derechos humanos llevadas a cabo por Israel en Gaza y en la Cisjordania ocupada mientras ven peligrar su trabajo y su vida. El colectivo de trabajadoras de medios de comunicación y periodistas ha sido uno de los colectivos objetivo de la guerra en Gaza por parte de Israel[321]. A finales de septiembre de 2024, 128 periodistas y personal de medios de comunicación habían sido asesinados en Gaza de acuerdo con el CPJ (Committee to Protect Journalists)[322]. Uno de los casos paradigmáticos de hostigamiento y control israelí sobre periodistas e influencers es el del palestino Motaz Azai-

318 **Guerrero, M.** "Israel's largest weapons manufacturer to help expand Us's virtual border wall." TruthOut. 24 de julio de 2024.
Disponible en:
https://truthout.org/articles/israels-largest-weapons-manufacturer-to-help-expand-uss-virtual-border-wall

319 **Verfassungsblog.** "Gaza, Artificial Intelligene and Kill Lists." 16 de mayo de 2024.
Disponible en: https://verfassungsblog.de/gaza-artificial-intelligence-and-kill-lists/

320 **El Salto Diario.** "Ciberactivismo." 29 de junio de 2024.
Disponible en: https://www.elsaltodiario.com/analisis/digitine-ciberactivismo-movimiento-pro-palestina

321 **The Gaza Project.** "The destruction of press infrastructure in Gaza." 2024.
Disponible en: https://arij.net/investigations/gaza-project/en/targeting-media-institutions/index.html

322 **Committee to protect journalists.** "Journalists casualties in the Israel-Gaza War." 12 de septiembre de 2024.
Disponible en: https://cpj.org/2024/07/journalist-casualties-in-the-israel-gaza-conflict/

za[323] de Gaza, que después de más de 100 días documentando el genocidio de Gaza tuvo que ser evacuado a Qatar por razones de seguridad[324]. Otro caso relevante es el de Bisan Owda, periodista palestina que recientemente recibió un premio por mostrar los ataques y la realidad de lo que sucede en Gaza[325].

2. SISTEMA DE RECONOCIMIENTO FACIAL[326] Y VIGILANCIA BIOMÉTRICA

La invasión terrestre de Gaza por parte de Israel ha sido una oportunidad para ampliar la vigilancia biométrica de las personas palestinas ya desplegada en Cisjordania y Jerusalén Este. El New York Times informó sobre cómo el ejército israelí está utilizando un amplio sistema de reconocimiento facial en Gaza «para llevar a cabo una vigilancia masiva allí, recogiendo y catalogando los rostros de las palestinas sin su consentimiento»[327]. Según esta información, este sistema utiliza tecnología de la empresa israelí Corsight y Google Photos para seleccionar rostros de multitudes e incluirlas en una base de datos. Corsight ha desarrollado una aplicación de reconocimiento facial basada en IA que es utilizada por el ejército israelí para vigilar a la población palestina en Gaza[328]. Además, el ejército israelí también ha establecido puestos de control a lo largo de las principales carreteras que la población palestina estaba utilizando para huir de las zonas donde se producían los ataques más intensos, con cámaras que

"La invasión terrestre de Gaza por parte de Israel ha sido una oportunidad para ampliar la vigilancia biométrica de las personas palestinas, ya desplegada en Cisjordania y Jerusalén Este"

323 **Journalism Festival.** "Motaz Azaiza."
Disponible en: https://www.journalismfestival.com/speaker/motaz-azaiza

324 **McKernan.** "Palestinian journalist leaves Gaza after 108 days chronicling war." The Guardian. 26 de enero de 2024.
Disponible en:
https://www.theguardian.com/world/2024/jan/26/palestinian-journalist-motaz-azaiza-leaves-gaza-qatar

325 **Peabody Awards.** "It's Bisan from Gaza." Peabody Awards.
Disponible en: https://peabodyawards.com/award-profile/its-bisan-from-gaza/

326 Ver glosario.

327 **The New York Times.** "Israel deploys expansive facial recognition program in Gaza." 2024.
Disponible en: https://www.nytimes.com/2024/03/27/technology/israel-facial-recognition-gaza.html

328 **The Verge.** "Israel is using mass facial recognition program in the Gaza Strip." 2024.
Disponible en:
https://www.theverge.com/2024/3/27/24114043/israel-facial-recognition-gaza-strip-corsight_

escaneaban los rostros[329].También se está utilizando la tecnología de Alphabet, empresa subsidiaria de Google, ya que el ejército israelí utiliza la función de reconocimiento facial de Google Photos como parte de la vigilancia y control total de la población palestina en Gaza. Además de estos servicios, Google ha ampliado su colaboración con el Ministerio de Defensa israelí al ofrecer un espacio seguro en la nube para procesar y almacenar todo tipo de datos[330].

El aislamiento de Gaza no solo se ha producido de forma tecnológica, sino que también ha habido empresas que llevan generando beneficios año tras año gracias a la construcción de vallas inteligentes, es decir, que incluyen sensores de movimiento y tecnología biométrica y que separan Gaza del Estado de Israel. En este sentido, la empresa Magal Security ejerce un rol fundamental[331]. Otro de los contextos en los que es posible recoger más información, tanto personal como biométrica, es en los checkpoints militares o puestos de control impuestos por Israel. La empresa Anyvision, renombrada en 2021 como Oosto[332], colabora con el ejército israelí en un sistema instalado en los puestos de control militares israelíes en la Cisjordania ocupada que utiliza la tecnología de reconocimiento facial[333] de la compañía para la identificación de permisos de trabajo. En septiembre de 2020, Anyvision completó el establecimiento de SightX, proyecto que comparte con el fabricante de armas israelí Rafael Advanced Defense Systems[334] [335]. SightX implementa tecnologías avanzadas de detección y seguimiento utilizando inteligencia artificial y basadas en la tecnología de visión artificial desarrollada por Anyvision con fines militares[336].

329 **The New York Times.** "Israel deploys expansive facial recognition program in Gaza." The New York Times. (2024). Disponible en: https://www.nytimes.com/2024/03/27/technology/israel-facial-recognition-gaza.html

330 **Time.** "Google contract shows deal with the Israel Defence Ministry." 2024. Disponible en: https://time.com/6966102/google-contract-israel-defense-ministry-gaza-war/

331 **+972 Magazine**. "Israel arms companies that will profit from the last assault in Gaza." 2022. Disponible en: https://www.972mag.com/israeli-arms-companies-surveillance-gaza/

332 **Who Profits.** "Ficha Anyvision." Disponible en: https://www.whoprofits.org/companies/company/6872/ar

333 Ver glosario.

334 **Business and Human Rights Resource Center.** "Anyvision raises concerns." 28 de septiembre de 2022. Disponible en: https://www.business-humanrights.org/es/%C3%BAltimas-noticias/privacy-and-discrimination-concerns-over-anyvision-facial-recognition-technology-at-palestine-checkpoints-company-did-not-respond/

335 **Who Profits.** "Israel Aerospace Industries (IAI)." Disponible en: https://www.whoprofits.org/companies/company/6872/ar.

336 Ibid.

3. REPRESIÓN TECNOLÓGICA Y CONTROL DE LAS COMUNICACIONES

El espionaje sobre defensoras de derechos humanos es una tendencia preocupante que afecta directamente al derecho a la privacidad y al secreto de las comunicaciones, entre otros. En este sentido, en noviembre de 2021 se descubrió que al menos a seis defensoras palestinas de derechos humanos les habían hackeado el teléfono a través del software Pegasus[337]. Justo después de la infiltración en los dispositivos de defensoras de derechos humanos el Gobierno de Israel incluyó a seis organizaciones no gubernamentales palestinas que desarrollaban su trabajo en Cisjordania, dentro del listado de organizaciones terroristas.

Otra tendencia alarmante documentada es el arresto e interrogatorio de palestinas por sus actividades en las redes sociales. Han surgido numerosos casos en los que se ha detenido a personas simplemente por expresar sus puntos de vista u opiniones en diversas plataformas digitales[338]. Además de este férreo control de las redes sociales, el ejército israelí inspecciona de forma sistemática los teléfonos móviles de las palestinas en Jerusalén Este, produciéndose a menudo detenciones arbitrarias o acoso[339]. Una defensora de derechos humanos palestina entrevistada recientemente en el marco de un encuentro internacional, compartía que "mientras utilizo mi teléfono móvil al hablar con alguna persona allegada, escucho voces de otras personas, tenemos que adaptar el lenguaje y adoptar capas de protección de cifrado en nuestros dispositivos móviles"[340].

Los bombardeos que tienen lugar durante el genocidio actual han dañado la infraestructura de telecomunicaciones, provocando apagones totales y parciales en la Franja de Gaza. También han provocado deliberadamente cortes de electricidad que han comprometido aún más la conectividad de toda la región. Desde el comienzo del genocidio, las autoridades israelíes han utilizado los apagones de Internet como herramienta de castigo colectivo a través de una serie de tácticas, como la imposición de apagones intermitentes de las comunicaciones que coinciden con intensos bombardeos, la destrucción de la infraestructura de telecomunicaciones, el corte del tráfico a los provee-

337 **Amnesty International.** "Devices of Palestinian HHRR defenders hacked." 8 de noviembre de 2021. Disponible en: https://www.amnesty.org/en/latest/research/2021/11/devices-of-palestinian-human-rights-defenders-hacked-with-nso-groups-pegasus-spyware-2/

338 **Adalah**. "Adalah monitorea las violencias de la guerra." 27 de octubre de 2023. Disponible en: https://www.adalah.org/ar/content/view/10939

339 **7amleh.** "Briefing on the Palestinian Digital Rights Situation since October 7th 2023." 2023. Disponible en: https://7amleh.org/2023/11/01/briefing-on-the-palestinian-digital-rights-situation-since-october-7th-2023

340 Defensora de derechos humanos palestina, entrevista realizada en el marco de The Nonviolence Factory, noviembre de 2023. Equipo NOVACT, SUDS, IRIDIA y ODHE.

dores de servicios de Internet (ISP) y el bloqueo del acceso al combustible necesario para alimentar los servicios de telecomunicaciones[341]. En conjunto, estos cierres han mantenido a la población de Gaza casi por completo desconectada y la han aislado gravemente[342].

Desde el 7 de octubre de 2023, las defensoras de derechos humanos, influencers y blogueras palestinas se han enfrentado a una mayor censura en línea. Esta censura ha sido particularmente fuerte en las plataformas propiedad de Meta[343], Facebook e Instagram[344], aunque también en otras plataformas como X[345] (antigua Twitter) o Telegram donde las defensoras de derechos humanos han documentado el silenciamiento sistemático de las voces palestinas a través de la eliminación arbitraria de contenidos[346], la suspensión de cuentas palestinas y las restricciones a los usuarios y contenidos propalestinos.

"Desde el comienzo del genocidio, las autoridades israelíes han utilizado los apagones de Internet como herramienta de castigo colectivo a través de una serie de tácticas, como la imposición de apagones intermitentes de las comunicaciones que coinciden con intensos bombardeos, la destrucción de la infraestructura de telecomunicaciones, el corte del tráfico a los proveedores de servicios de Internet (ISP) y el bloqueo del acceso al combustible necesario para alimentar los servicios de telecomunicaciones"

341 **Access Now.** "Palestine Unplugged: how Israel disrupts Gaza's internet." 2024. Disponible en: https://www.accessnow.org/publication/palestine-unplugged/

342 **Access Now.** "Shrinking democracy, growing violence." 2024. Disponible en: https://www.accessnow.org/wp-content/uploads/2024/05/2023-KIO-Report.pdf

343 **Access Now.** "How Meta censors Palestinian voices." 2024. Disponible en: https://www.accessnow.org/publication/how-meta-censors-palestinian-voices/

344 **HRW Report.** "Meta's broken promises." 2023. Disponible en: https://www.hrw.org/report/2023/12/21/metas-broken-promises/systemic-censorship-palestine-content-instagram-and

345 **Business and Human Rights Resource Centre.** "X Allegedly suspends hundreds of Palestinian accounts." 2023. Disponible en: https://www.business-humanrights.org/en/latest-news/x-allegedly-suspends-hundreds-of-palestinian-accounts-amid-israel-gaza-war/

346 **7Amleh.** "Briefing on the Palestinian Digital Rights Situation." 2024. Disponible en: https://7amleh.org/2023/11/01/briefing-on-the-palestinian-digital-rights-situation-since-october-7th-2023

VIII

JORDANIA: LA DERIVA A LA AUTOCENSURA

El panorama político de Jordania, considerado un "Caballo de Troya" en el Mashreq[347], ha experimentado una importante transformación en la última década. Este cambio se ha visto especialmente influido por la Primavera Árabe, la actual pandemia de COVID-19 y diversos acontecimientos sociopolíticos posteriores. Un elemento central de estos cambios ha sido la creciente dependencia del Gobierno jordano a la vigilancia masiva como herramienta para mantener el control político y el orden público.

El entorno político de Jordania se ha caracterizado por una mezcla de monarquía tradicional y estructuras estatales modernas, con el rey Abdalá II al frente. Las Primaveras Árabes trajeron a Jordania oleadas de protestas antigubernamentales[348] que al principio fueron respondidas con promesas de reforma y mayores libertades por parte de la monarquía. Sin embargo, estas promesas pronto se vieron eclipsadas por estrictas medidas destinadas a frenar la disidencia. En 2013, por ejemplo, el Gobierno jordano bloqueó 304 sitios web de noticias en virtud de una controvertida ley de publicación, medida que se consideró un ataque directo a la libertad de prensa[349].

La Dirección General de Inteligencia (GID) (también conocida como "mukhabarat") ha desempeñado un papel central en estas actividades de vigilancia, aprovechando tecnologías avanzadas[350].

La introducción de la Ley de Ciberdelincuencia en 2015 marcó un importante punto de inflexión en los esfuerzos del Gobierno por controlar las comunicaciones digitales[351]. Esta ley, que incluye cargos como "difundir noticias falsas" e "incitar a la violencia", se ha utilizado con frecuencia para procesar a periodistas y defensoras de derechos humanos. Esta herramienta legal ha permitido al Gobierno ejercer un mayor control sobre las actividades en línea, lo que ha provocado un aumento de la censura y la autocensura entre quienes se atreven a alzar sus voces[352].

347 La noción de "caballo de Troya" sugiere que Jordania podría estar desempeñando un papel oculto o estratégico en beneficio de intereses externos o diferentes a los que aparenta, en una región caracterizada por tensiones políticas. Esto implica que Jordania podría estar facilitando la entrada o influencia de potencias externas en Oriente Medio de manera discreta.

348 **Gupta, Saumyaa; Spring, Jordan**. "An Analysis of the Regime Survival Tactics Adopted by the Hashemite Kingdom." Independent Study Project, SIT Graduate Institute. 2023.
Disponible en: https://digitalcollections.sit.edu/cgi/viewcontent.cgi?article=4619&context=isp_collection

349 **Jamal Halaby.** "Jordan: 304 national news website blocked." AP News. 3 de junio de 2013.
Disponible en: https://apnews.com/article/b1b0f9f29a5d4368b7a97792b76570ce

350 **Yahia Sukkeir.** "Jordan," "Global Information Society Watch." 2014.
Disponible en: https://giswatch.org/en/country-report/communications-surveillance/jordan

351 **Dentons.** "Cybercrime Law in Jordan." 16 de octubre de 2023.
Disponible en: https://www.dentons.com/en/insights/alerts/2023/october/16/cybercrime-law-in-jordan

352 **Sukkeir, Yahia**. "Jordan. Global Information Society Watch." 2014.
Disponible en: https://giswatch.org/en/country-report/communications-surveillance/jordan

1. BLOQUEO DE INTERNET PARA SILENCIAR VOCES DISIDENTES Y NEUTRALIZAR LA MOVILIZACIÓN SOCIAL

En los últimos años, el Gobierno jordano ha actuado de forma contundente para cerrar sitios web de noticias independientes, una clara demostración de su estrategia con el control del flujo de información y la represión de las disidencias. Esta acción se ejecuta principalmente en virtud de la controvertida Ley de Prensa y Publicaciones de 2013[353], cuyo objetivo aparente es impedir la difusión de información falsa y mantener la seguridad nacional. Sin embargo, en la práctica, esta ley se ha utilizado para suprimir cualquier forma de medio de comunicación que no se alinee con la narrativa del Gobierno, socavando significativamente la libertad de prensa en el país. La persecución colectiva de los medios de comunicación independientes ha tenido un profundo impacto en el panorama de los medios de comunicación en Jordania.

La nueva Ley de Ciberdelincuencia, a través de su artículo 37, permite al Gobierno cerrar, bloquear páginas web y aplicaciones que no respetan dicha ley[354]. Plataformas como Tik Tok, Clubhouse, Facebook live, Al-Hudood o 7iber han sido bloqueadas temporalmente. Según fuentes gubernamentales, estas plataformas y aplicaciones fueron bloqueadas por presuntamente difundir desinformación o incitar a la violencia[355]. Sin embargo, las plataformas fueron bloqueadas durante movilizaciones masivas en el país, como la huelga de las profesoras en 2020 o la de camioneras en la ciudad de Maan en 2022, para evitar que defensoras de derechos humanos pudieran difundir imágenes y noticias sobre estas protestas[356]. Además, Jordania es uno de los países de la región que más demandas de información realiza a las grandes empresas de redes sociales. Agencias como la Comisión de Medios Jordanos, la Comisión Regulatoria de Telecomunicaciones u otras agencias de seguridad tienen competencias para cerrar y suspender temporalmente estas páginas web.

Esta censura digital se realiza a través de diversas estrategias que incluyen el uso de tecnologías avanzadas de control de internet. La tecnología utilizada para aplicar estas

353 **Al Tamimi & Company.** "Jordan's Amendments to the Press and Publications Law." Law Update. Disponible en: https://www.tamimi.com/law-update-articles/jordans-amendments-to-the-press-and-publications-law.

354 **Salam Freihat.** "Jordan's Cybercrime Law to Limit Investments and E-commerce," *SMEX*. 30 de Agosto 2023. Disponible en: https://smex.org/jordans-cybercrime-law-to-limit-investments-and-e-commerce/

355 **Abdullah Jbour.** "Jeopardizing Digital Rights in Jordan" *Carnegie Endowment for International Peace*. 15 agosto de 2023. Disponible en: https://carnegieendowment.org/sada/2023/08/jeopardizing-digital-rights-in-jordan?lang=en

356 **SMEX.** "Jordan: How Are Users Affected by the TikTok Ban?" *SMEX*. 25 de mayo de 2023. Disponible en: https://smex.org/jordan-how-are-users-affected-by-the-tiktok-ban/

medidas incluye sofisticados sistemas de filtrado de Internet como la DPI[357] que bloquean URL y contenidos específicos basándose en palabras clave y otros indicadores[358]. Una empresa estadounidense ha desarrollado e implantado el programa Smart Filter en Jordania[359], que permite al Gobierno filtrar y bloquear contenidos en línea considerados inapropiados o una amenaza para la seguridad nacional. Este programa se ha utilizado para censurar contenidos en línea, restringiendo el acceso a la información y coartando la libertad de expresión[360]. El uso de este programa se intensificó notablemente tras el COVID-19. Además, las proveedoras de servicios de Internet también están obligadas a cumplir las directivas gubernamentales para bloquear el acceso a determinados sitios web y vigilar las actividades en línea de las usuarias, garantizando la aplicación exhaustiva de estas medidas de censura[361].

2. HACKEO MASIVO DEL PERIODISMO INDEPENDIENTE

La persecución de periodistas y profesionales que intentan trabajar al margen de la estricta normativa del Gobierno es también una práctica habitual en Jordania. La Ley de Ciberdelincuencia, la Ley de Telecomunicaciones y la Ley de Prevención de Delitos son las principales herramientas empleadas para criminalizar a estas profesionales, ya que permiten eludir los procedimientos judiciales habituales, permitiendo a las Fuerzas de Seguridad del Estado detener a personas sin supervisión judicial[362]. La Ley de Ciberdelincuencia, en particular sus artículos 15 y 17, ha sido una herramienta clave para criminalizar a periodistas y personal de los medios de comunicación, otorgando al Gobierno amplios poderes discrecionales para suprimir la libertad de prensa.

Entre los casos más relevantes, destaca el encarcelamiento de la periodista Hiba Abu Taha, por una denuncia presentada por la Comisión de Medios de Comunicación el 13 de mayo de 2024 en base a los artículos 15 y 17 de la Ley de Ciberdelincuencia. Inicialmente, el presunto cibercrimen se basaba en la publicación de un informe de investigación en el

357 Ver glosario.

358 **AlAshry, Miral Sabry.** "Arab authorities use digital surveillance to control press freedom: journalists' perceptions." 2021.
Disponible en: https://safetyofjournalists.org/assets/studies/10_1108_dprg_05_2021_0071__1_.pdf

359 Ibid. p. 9

360 Ibid. p.10.

361 **Privacy International.** "State of Privacy Jordan." 2019.
Disponible en: https://www.privacyinternational.org/state-privacy/1004/state-privacy-jordan

362 **Office of the United Nations High Commissioner for Human Rights**. "Detention of Activists in Jordan." 27 de abril de 2022.
Disponible en: https://www.ohchr.org/en/press-releases/2022/04/detention-activists-jordan

medio Annasher donde describía las relaciones de complicidad entre el Gobierno jordano e israelí en el genocidio de Gaza, a través del establecimiento de un corredor terrestre entre los dos países para el suministro de materiales a Israel[363]. Sin embargo, posteriormente se descubrió que la acusación se centraba en otro artículo donde Taha criticaba al Gobierno jordano por permitir a Israel el uso de su espacio aéreo para interceptar los misiles de Irán[364]. A pesar de los esfuerzos por conseguir su liberación, Hiba permanece aún detenida en la prisión de Juwaida[365]. Otro caso similar es el de una estudiante de periodismo, que se enfrenta a una deportación inminente a Siria a pesar de estar registrada como solicitante de asilo en ACNUR desde 2013. Su arresto el 9 de abril de 2024, mientras filmaba una manifestación, y su posterior detención sin procedimiento judicial, ponen de relieve el uso de la Ley de Prevención de Delitos para eludir los procesos legales habituales[366]. El caso de Abdul Jabbar Zeitoun refleja la discrecionalidad de las Fuerzas de Seguridad del Estado. Zeitoun, fotoperiodista independiente, fue detenido durante una semana en marzo de 2024 mientras cubría unas protestas contra la guerra, a pesar de haberse identificado inmediatamente como periodista en el momento de su detención[367].

Las mujeres periodistas son especialmente vulnerables, y se enfrentan al acoso, la intimidación y la persecución. Una persona fue multada con 5.000 dinares en virtud de la Ley de Ciberdelincuencia por difundir supuestamente noticias falsas y difamar a instituciones oficiales. Detenida inicialmente en diciembre de 2023, fue puesta en libertad más tarde, y la multa se anuló finalmente en virtud de una ley de amnistía[368]. La persecución personal y colectiva de periodistas y medios de comunicación ha creado un clima de miedo y represión, en el que los riesgos de denunciar son elevados y las vías para hacerlo son cada vez más limitadas. Según el experto en comunicación Mohammed Shamma: "debido a este clima de represión, la gente a mi alrededor tiene miedo y para evitar cualquier ataque, se auto-

"debido a este clima de represión, la gente a mi alrededor tiene miedo y para evitar cualquier ataque, se autocensura, reduciendo su activismo y su actividad en las redes sociales"

363 **Committee to Protect Journalists.** "Palestinian-Jordanian Journalist Hiba Abu Taha Sentenced to One Year in Prison." 6 de junio de 2024.
Disponible en: https://cpj.org/2024/06/palestinian-jordanian-journalist-hiba-abu-taha-sentenced-to-one-year-in-prison

364 **Hiba Abu Tahar.** "دور الأردن في الدفاع عن كيان العدو," Annasher. 22 de abril de 2024.
Disponible en: https://annasher.com/exclusive/12857/

365 Acceso a manuscrito aún no publicado. Mohammed Shamma, *Report on Journalist Detentions and media violations in Jordan.* Reporters Without Borders, Amman, 2024.

366 Ibid.

367 Ibid.

368 Ibid.

censura, reduciendo su activismo y su actividad en las redes sociales"[369].

La tecnología de la empresa israelí NSO Group ha sido esencial para la represión del periodismo independiente en Jordania. Según un informe de Access Now, entre 2019 y 2023, 35 defensoras de derechos humanos y líderes políticas, de las cuales 16 eran periodistas, fueron atacadas digitalmente con el *spyware*[370] Pegasus de NSO Group.[371] Entre las periodistas afectadas destacan dos periodistas del Organized Crime and Corruption Reporting Project, el fotoperiodista y documentalista independiente Abdul Jabbar Zeitoun que fue detenido el 21 de marzo de 2024 durante unas protestas contra la guerra o la mencionada periodista Hiba Abu Taha. Según Mohammed Shamma: "el objetivo es silenciar voces y reprimir a defensoras de derechos humanos y periodistas a través de leyes y tecnologías que se utilizaron durante el periodo del virus Corona"[372]. Pegasus siguió siendo un componente fundamental de la estrategia de vigilancia de Jordania tras el COVID-19.

3. VIOLENCIA DIGITAL CONTRA DEFENSORAS DE LOS DERECHOS HUMANOS Y PERSONAS LGBTIQ+

El clima sociopolítico de Jordania ha sido testigo de una creciente represión de las defensoras de los derechos humanos, caracterizada por detenciones, intimidaciones y vigilancia, todo ello justificado al amparo de amplios marcos legales como el Código Penal, la Ley de Ciberdelincuencia y la Ley Antiterrorista de 2006[373]. La comunidad LGTBIQ+ se encuentra entre los colectivos más afectados por el control y la represión institucional. En el panorama jordano se han producido cada vez más detenciones e intimidaciones de personas LGBTIQ+ también en virtud del Código Penal y de la Ley Antiterrorista especialmente. Casos notables son la detención del director de un centro LGBTIQ+, arrestado por la policía, y la detención de defensoras de derechos humanos bajo vagas acusaciones de

369 Mohammed Shamma, entrevista personal realizada por el equipo de investigación, 25 de junio de 2024.

370 Ver glosario.

371 **Access Now.** "Between a Hack and a Hard Place: How Pegasus Spyware Crushes Civic Space in Jordan" 2024. Disponible en: https://www.accessnow.org/publication/between-a-hack-and-a-hard-place-how-pegasus-spyware-crushes-civic-space-in-jordan/

372 Mohammed Shamma, entrevista personal realizada por el equipo de investigación, 25 de junio de 2024.

373 **Office of the United Nations High Commissioner for Human Rights.** "Detention of Activists in Jordan." 29 de abril de 2022.
Disponible en: https://www.ohchr.org/en/press-releases/2022/04/detention-activists-jordan.

poner en peligro la seguridad nacional[374]. La experta en comunicación Yara Harare afirma que el Gobierno ataca derechos civiles y políticos para anular el espacio cívico y atacar cualquier grupo que intente transformar la sociedad jordana. En este sentido, Harare añade que la comunidad LGBTIQ+ está siendo especialmente reprimida, provocando miedo y autocensura entre sus activistas, llegando al extremo de no poder mencionar públicamente palabras como LGBTIQ+ o queer[375].

La infraestructura tecnológica forma parte de una estrategia más amplia de vigilancia y control de las comunicaciones digitales, que incluye la vigilancia de las usuarias de los cibercafés y el registro obligatorio de la tarjeta SIM. En este sentido, se introdujeron normativas que obligan a los cibercafés a mantener registros detallados de las identidades de las usuarias, vigilar las actividades mediante cámaras de seguridad y registrar los sitios web visitados[376]. Mientras el registro obligatorio de las tarjetas SIM con los datos del documento nacional de identidad o del pasaporte, incluidos los datos biométricos, ha facilitado una amplia vigilancia de las telecomunicaciones[377]. Este requisito ha permitido a las autoridades el rastreo y la interceptación de las comunicaciones, coartando aún más el anonimato y la libertad de expresión.

Este sistema de vigilancia masiva tiene un impacto directo en la libertad de expresión y el espacio cívico en Jordania. Destacadas defensoras de los derechos humanos, como el abogado Malik Abu Orabi, fue objeto de repetidos ataques con el programa espía Pegasus entre agosto de 2019 y julio de 2021[378]. Ahmad Al-Neimat, defensor de los derechos humanos y activista contra la corrupción, sufrió el hackeo de su teléfono en enero de 2021 y se enfrentó a repetidas detenciones[379]. Lama Fakih, directora para Oriente Medio y el Norte de África de Human Rights Watch, vio infectado su iPhone cinco veces con el programa espía Pegasus entre abril y agosto de 2021, e Hiba Zayadin, investigadora principal de Human Rights Watch, recibió múltiples notificaciones de Apple en 2023 informando que su móvil estaba siendo atacado por *spyware*[380] patrocinados por

374 **William Christou,** "Jordan's Secret Police Accused of Targeting LGBTQ+ Community" *The Guardian*. 18 de agosto de 2023. sec. Global development.
Disponible en:
https://www.theguardian.com/global-development/2023/aug/18/jordans-secret-police-accused-of-targeting-lgbtq-community

375 Yara Harare, entrevista personal realizada por el equipo de investigación, 14 de junio de 2024.

376 **Privacy International.** "State of Privacy: Jordan." 2019.
Disponible en: https://privacyinternational.org/state-privacy/1004/state-privacy-jordan

377 Ibid.

378 **Front Line Defenders.** "Profile: Malik Abu Orabi."
Disponible en: https://www.frontlinedefenders.org/en/profile/malik-abu-orabi.

379 **Front Line Defenders**. *Jordanian Human Rights Defenders Ahmed Al-Neimat and Abdulrahman Shdaifat Prevented from Travelling*. 14 de octubre de 2021.
Disponible en:
https://www.frontlinedefenders.org/en/case/jordanian-human-rights-defenders-ahmed-al-neimat-and-abdulrahman-shdaifat-prevented-travelling.

380 Ver glosario.

agentes gubernamentales[381]. Este entorno represivo fomenta la autocensura y el miedo entre periodistas, defensoras de derechos humanos y personas LGBTIQ+, socavando las libertades civiles y los valores democráticos en Jordania[382]. Según Yara Harare, Jordania es líder en el encubrimiento de los casos de persecución de activistas: "Hay un apagón informativo sobre estos casos a nivel internacional"[383].

"Jordania es líder en el encubrimiento de la persecución de activistas. Existe un apagón informativo sobre estos casos a nivel internacional"

4. VIGILANCIA Y REPRESIÓN DE LAS PROTESTAS CONTRA EL GENOCIDIO EN GAZA

La censura de la información militar y de seguridad en Jordania se ha intensificado significativamente desde octubre de 2023, lo que refleja los continuos esfuerzos del Gobierno por controlar la información y suprimir cualquier forma de disidencia en relación con sus operaciones de seguridad y sus implicaciones en el actual conflicto de Gaza. Las principales herramientas jurídicas que facilitan esta censura y represión son la Ley de Ciberdelincuencia, en particular sus artículos 15 y 17, y la Ley de Prevención de Delitos.

Los ataques indiscriminados de Israel contra la población de Gaza provocaron en Jordania una gran indignación que desembocó en espontáneas y multitudinarias manifestaciones ante la Embajada israelí en el distrito de Rabyeh en Ammán. Mohammed Shamma ha documentado, durante el 2024, 11 casos de obstrucción de la actividad de periodistas, incluyendo en algunos casos detenciones, por cubrir las manifestaciones pro-palestinas[384]. Algunos casos relevantes son Khair Eddine Al Jabri que fue detenido en marzo de 2024 en virtud de la Ley de Ciberdelincuencia por volver a publicar un videoclip que criticaba

381 **Human Rights Watch**, "Spyware Targets Human Rights Watch Staff in Jordan," *Human Rights Watch*. 1 de febrero de 2024.
Disponible en: https://www.hrw.org/news/2024/02/01/spyware-targets-human-rights-watch-staff-jordan.

382 **William Christou**, "Jordan's Secret Police Accused of Targeting LGBTQ+ Community," *The Guardian*. 18 de agosto de 2023.
Disponible en:
https://www.theguardian.com/global-development/2023/aug/18/jordans-secret-police-accused-of-targeting-lgbtq-community

383 Yara Harare, entrevista personal realizada por el equipo de investigación, 14 de junio de 2024.

384 Mohammed Shamma, entrevista personal realizada por el equipo de investigación, 25 de junio de 2024.

la actuación de las fuerzas policiales en las protestas por Gaza[385]. Un fotoperiodista, fue detenido durante casi un mes en marzo de 2024 mientras cubría las protestas en la zona de Rabyeh. A pesar de la decisión del fiscal de ponerlo en libertad, el gobernador insistió en encarcelarlo, lo que indica una actitud punitiva hacia la información sobre sucesos relacionados con la seguridad[386]. Por último, una realizadora audiovisual fue presionado por la GID en marzo de 2024 para que firmara un compromiso de no participar en protestas, como las pro-palestinas, que significan una amenaza para la seguridad nacional del país. Estos casos ponen de relieve una pauta de utilización de marcos jurídicos como la Ley de Ciberdelincuencia y la Ley de Prevención de Delitos para reprimir a las disidencias y vigilar a la sociedad civil[387].

Para la obstrucción y persecución de la actividad periodística se utiliza un exhaustivo monitoreo de las redes sociales para identificar contenidos digitales y el control y seguimiento en las manifestaciones. La Comisión de Medios de Comunicación y la GID están siendo agencias relevantes en esta vigilancia masiva. Sin embargo, se desconoce quién está gestionando la captura de imágenes a través de cámaras de videovigilancia que han sido colocadas de forma estratégica en la zona de protesta en Rabyeh. Según indica una investigadora de la Jordan Open Source Association, estas cámaras son diferentes de las cámaras para el control de tráfico que se pueden encontrar en la ciudad de Amman y que capturan imágenes gestionadas por el Centro de Control de Tráfico bajo el control de la Dirección de Seguridad Pública y Protección Civil[388].

385 Acceso a manuscrito aún no publicado. Mohammed Shamma, *Report on Journalist Detentions and media violations in Jordan*, Reporters Without Borders, Amman, 2024.

386 Ibid.

387 Ibid.

388 **Yara AlRafie**, "Public Cameras/CCTV Amman", Jordan Open Source Association. 21 de Agosto de 2022. Disponible en: https://www.josa.ngo/blog/217

IX

IRAK: LA MILITARIZACIÓN DEL ESPACIO DIGITAL

En octubre de 2019, miles de manifestantes tomaron las calles de Bagdad y otras ciudades del sur del país en contra de la corrupción del Gobierno. A pesar del carácter no violento del movimiento social Tishreen[389], las Fuerzas de Seguridad Iraquíes y milicias vinculadas con el Gobierno, asesinaron a alrededor de 500 personas en los primeros 7 meses de la revuelta popular[390]. La represión se trasladó también a los espacios digitales donde las publicaciones de apoyo a las movilizaciones implicaron arrestos fulminantes por agentes de unidades antiterroristas[391]. Desde 2003, Irak ha ido derivando en uno de los Gobiernos más restrictivos de la región Mashreq con un marco legal que ataca las libertades civiles de la sociedad.

La persecución de la disidencia política en Irak ha sido una práctica común desde el periodo colonial británico y el régimen de Saddam Hussein. Con la caída del dictador, se produce una apertura del espacio cívico con miles de organizaciones no gubernamentales y medios de comunicación registrados en el país. Entre 2003 y 2019, se crearon más de 200 nuevas estaciones de radio en Irak[392]. Paralelamente, los servicios de inteligencia iraquíes fueron también modernizados por Estados Unidos y Reino Unido para luchar contra la insurgencia en el país[393]. A partir de la derrota del Daesh (Estado Islámico de Irak y Siria) en 2017, las tecnologías de vigilancia pasan a utilizarse en otras esferas de la seguridad nacional para defender los valores de la nación. En la práctica esto se tradujo en un aumento de la vigilancia masiva de defensoras de derechos humanos y periodistas en el país[394]. Se calcula que 1,3 millones de personas en Irak están en riesgo de violencia digital, el 75% de las cuales son mujeres y niñas[395].

---

389 Movimiento Tishreen es como se ha denominado al movimiento social que surgió durante las protestas iraquíes de 2019-2021. El principal centro de las protestas fue la plaza Tahrir de Bagdad, con otras protestas que tuvieron lugar en Basora y Nayaf.

390 **UNAMI.** "Human Rights Violations and Abuses in the Context of Demonstrations in Iraq. October 2019 to April 2020." 2020.
Disponible en:
https://www.ohchr.org/sites/default/files/Documents/Countries/IQ/Demonstrations-Iraq-UNAMI-OHCHR-report.pdf

391 **Human Rights Watch.** "Iraq: Arrests for Voicing Protest Solidarity." 4 de noviembre de 2019.
Disponible en: https://www.hrw.org/news/2019/11/04/iraq-arrests-voicing-protest-solidarity

392 **Aso Q. Abdullah, Sangar Y. Salih, and Jihad H. Mahmood.** "Invisible Threats: Digital Security and Female Journalists in Irak and the Kurdistan Region." 2020.
Disponible en:
https://www.researchgate.net/publication/360024571_Invisible_Threats_Digital_Security_and_Female_Journalists_in_Iraq_and_the_Kurdistan_Region

393 **U.S. Department of State.** "U.S. Security Cooperation with Iraq."
Disponible en: https://2017-2021.state.gov/u-s-security-cooperation-with-iraq-2/

394 **Aso Q. Abdullah, Sangar Y. Salih, and Jihad H. Mahmood.** "Invisible Threats: Digital Security and Female Journalists in Irak and the Kurdistan Region." 2020.
Disponible en:
https://www.researchgate.net/publication/360024571_Invisible_Threats_Digital_Security_and_Female_Journalists_in_Iraq_and_the_Kurdistan_Region

395 **Salamat MENA**. "Iraq: Domestic Violence Against Women Report 2023."
Disponible en: https://portal.salamatmena.org/wp-content/uploads/2024/01/Iraq-DVAW-2023-EN.pdf.

1. PRÁCTICAS ANTITERRORISTAS PARA NEUTRALIZAR LA DISIDENCIA POLÍTICA IRAQUÍ

La arquitectura de la seguridad nacional en Irak tiene un carácter predominantemente militar debido a décadas de lucha contra el terrorismo. En 2009, el primer ministro iraquí Nour Al-Maliki creó, con el apoyo de las agencias de inteligencia de la CIA y el MI6 británico, la Falcon Cell, una unidad de inteligencia especializada en la lucha contra el terrorismo y con poderes para investigar y neutralizar amenazas de seguridad nacional sin necesidad de órdenes judiciales. Por otro lado, el Gobierno norteamericano transfirió tecnología para monitorear y grabar llamadas telefónicas y mensajes de texto telefónicos con el objetivo de prevenir ataques terroristas[396]. Una de estas herramientas de espionaje pudo ser la tecnología Stingray: antenas simuladoras de telecomunicaciones que permiten interceptar comunicaciones móviles y generar sistemas de monitoreo de llamadas y SMS[397]. A mediados de 2023, el nuevo primer ministro Mohammed Shia Al-Sudani nombró a Abu Ali al-Basri, hasta entonces jefe de la Falcon Cell, como responsable de los Servicios de Seguridad Nacional Iraquí (INSS, por su acrónimo en inglés)[398].

El control de los servicios de inteligencia por parte de militares[399] y la aplicación de leyes y prácticas antiterroristas, han contribuido a representar a la disidencia política como una amenaza para la seguridad nacional. La Ley Antiterrorista nº13 de 2005 incluye ambigüedades en su definición de "acto terrorista" entendida como cualquier amenaza que atente

396 **Radio Free Europe.** "U.S. Providing Irak with Phone, SMS Monitoring Devices" *Radio Free Europe/Radio Liberty*. 21 de agosto de 2011.
Disponible en:
https://www.rferl.org/a/us_providing_Irak_with_phone_and_sms_monitoring_devices/24303623.html

397 **Michael Price.** "ICE Agents Are Using Battlefield Surveillance Technology to Snoop on Cell Phones", Brennan Center for Justice". 14 de junio de 2017.
Disponible en:
https://www.brennancenter.org/our-work/analysis-opinion/ice-agents-are-using-battlefield-surveillance-technology-snoop-cell

398 **Suadad al-Salhy.** "Irak: Sudani Shakes up Intelligence and Security Services in Political Power Play" *Middle East Eye*. 7 de julio de 2023.
Disponible en:
https://www.middleeasteye.net/news/iraq-sudani-shakes-intelligence-and-security-services-political-power-play

399 **Fawzi al-Zubaidi.** "Restructuring Iraki National Security Institutions in Sudani's Government", The Washington Institute". 25 de enero de 2023.
Disponible en:
https://www.washingtoninstitute.org/policy-analysis/restructuring-Iraki-national-security-institutions-sudanis-government

a la "unidad nacional"[400]. El Gobierno utilizó la ley antiterrorista para vigilar y arrestar a defensoras de derechos humanos de las movilizaciones de octubre de 2019, justificando que estas protestas eran violentas y alteraban el orden social del país. Por ejemplo, en la región de Anbar, algunas jóvenes fueron arrestadas por los servicios antiterroristas poco después de realizar publicaciones en Facebook donde mostraban su apoyo al movimiento Tishreen en 2019[401].

Los servicios de seguridad nacional iraquíes pueden obtener datos personales y contenidos de llamadas, mensajes y correos electrónicos, a través de las principales empresas de telecomunicaciones del país en casos de seguridad nacional. Se estima que alrededor de 40 millones de iraquíes están suscritos a contratos de móviles y 20 millones tienen suscripciones de internet con las dos principales empresas del país, Zain Irak y Asian Cell. Estas empresas están obligadas a dar datos personales como localización, mensajes y otro tipo de comunicaciones de sus usuarios si existe una autorización judicial. La interacción de estas empresas con la INSS para casos de seguridad nacional es muy frecuente[402].

En este sentido, un informe de 2020 de la Peace and Freedom Organization describe el aumento de la vigilancia masiva en periodos electorales[403]. El objetivo de la vigilancia es persuadir y/o neutralizar las voces disidentes a través de diferentes estrategias como la extorsión digital[404] o la violencia física. En los meses previos a las elecciones parlamentarias de 2021, varias defensoras de derechos humanos fueron asesinadas y más de 30 periodistas fueron arrestadas en la provincia de Dhi-Qar[405]. Concretamente, la persecución y represión de defensoras de derechos humanos de la ciudad de Nassiriyah, en Dhi-Qar, tenía el objetivo de controlar e intimidar a dos formaciones políticas opuestas al Gobierno como Imtidad y al-Bait al-Watani[406]. La persecución de la disidencia política continúa en la actualidad, también en la Región del Kurdistán Iraquí (KRI, por su acrónimo en inglés), con algunos casos muy recientes como la detención de Shakar Star, del medio Tiwar News, por parte de la agencia de inteligencia kurda Asayish, por presuntamente preparar y publicar

400 **Official Gazette of Iraq**. "Anti-Terrorism Law No. (13) of 2005." Disponible en: https://moj.gov.iq/upload/pdf/%D9%82%D8%A7%D9%86%D9%88%D9%86%20%D9%85%D9%83%D8%A7%D9%81%D8%AD%D8%A9%20%D8%A7%D9%84%D8%A7%D8%B1%D9%87%D8%A7%D8%A8%20-%20Copy.pdf.

401 **Human Rights Watch.** "Iraq: Arrests for Voicing Protest Solidarity." 2019. Disponible en: https://www.hrw.org/news/2019/11/04/iraq-arrests-voicing-protest-solidarity

402 **Tech 4 Peace.** "Privacy in Irak -Case of Telecommunication Companies". 2023. Disponible en: https://t4p-storage.eu-central-1.linodeobjects.com/y778AhwIUwAvopYJsFmHZxsxStpSfb39zOnEXc0t.pdf

403 **Aso Q. Abdullah, Sangar Y. Salih, and Jihad H. Mahmood.** "Invisible Threats: Digital Security and Female Journalists in Irak and the Kurdistan Region." 2020. Disponible en: https://www.researchgate.net/publication/360024571_Invisible_Threats_Digital_Security_and_Female_Journalists_in_Iraq_and_the_Kurdistan_Region

404 Ver glosario.

405 **Ali Al-Mikdam.** "The Ongoing Assassinations of Iraki Activists," The Washington Institute. 1 de julio de 2021. Disponible en: https://www.washingtoninstitute.org/policy-analysis/ongoing-assassinations-iraqi-activists

406 Ibid

un informe que se argumentó que incitaba a la violencia y a la desinformación[407].

La represión también ha conllevado asesinatos de defensoras de derechos humanos[408], detrás de los cuales estarían milicias armadas vinculadas con partidos políticos de Irak y el Gobierno de Irán. Entre ellas destacan las Fuerzas Movilización Popular (PMF, por su acrónimo en inglés), milicias predominantemente chiitas que fueron creadas para defender a las comunidades locales de la amenaza del Daesh. Sin embargo, en la actualidad, las PMF son responsables de ataques sistemáticos contra defensoras de derechos humanos y comunidades vulnerabilizadas[409]. Aunque el Gobierno iraquí ha intentado integrarlas en las Fuerzas y Cuerpos de Seguridad del Estado, continúan operando al margen de la ley. Por ejemplo, en 2020, Hisham al-Hashim, analista especializado en yihadismo, fue asesinado por un militante de la milicia pro-iraní Kataeb Hezbollah por sus críticas al Gobierno y los grupos armados no estatales[410].

2. APAGONES DIGITALES PARA DESARTICULAR LAS MOVILIZACIONES SOCIALES Y SILENCIAR LA VIOLENCIA INSTITUCIONAL

Irak es uno de los países del mundo que más utiliza la interrupción del acceso a internet como estrategia para silenciar el activismo político[411]. Desde 2019, el Gobierno bloqueó el acceso a internet en 126 ocasiones[412]. Muchos de estos apagones digitales se produjeron

407 **Committee to Protect Journalists.** "Iraqi Kurdish Asayish Security Forces Arrest Journalist Shakar Star After Smuggling Reports". 21 de mayo de 2024.
Disponible en:
https://cpj.org/2024/05/iraqi-kurdish-asayish-security-forces-arrest-journalist-shakar-star-after-smuggling-reports/

408 **Ali Al-Mikdam.** "The Ongoing Assassinations of Iraki Activists," The Washington Institute. 1 de julio de 2021.
Disponible en: https://www.washingtoninstitute.org/policy-analysis/ongoing-assassinations-iraqi-activists

409 **Shivan Fazil and Alaa Tartir.** "Irak in 2023: Challenges and Prospects for Peace and Human", SIPRI. 17 de mayo de 2023.
Disponible en:
https://www.sipri.org/commentary/topical-backgrounder/2023/Irak-2023-c7y6allenges-and-prospects-peace-and-human-security

410 **Agence France-Presse.** "Irak Court Sentences to Death Killer of Academic Hisham Al-Hashemi," Al-Monitor. 7 de mayo de 2023.
Disponible en
https://www.al-monitor.com/originals/2023/05/iraq-court-sentences-death-killer-academic-hisham-al-hashemi

411 **Access Now.** "Shrinking Democracy, Growing Violence. Internet Shutdowns in 2023,". Mayo de 2024.
Disponible en: https://www.accessnow.org/wp-content/uploads/2024/05/2023-KIO-Report.pdf

412 **Alex McDonald.** "Irak Had World's Largest Number of Internet Shutdowns in 2023 due to Exam Cheating," Middle East Eye. 9 de enero de 2024.
Disponible en:
https://www.middleeasteye.net/news/Irak-largest-number-internet-shutdowns-2023-over-cheating

“durante los períodos de bloqueo de internet, la violencia de la policía y las milicias contra las defensoras de derechos humanos aumenta, al no poderse difundir de inmediato imágenes y vídeos de esos ataques”

durante protestas sociales. Por ejemplo, durante las manifestaciones del movimiento Tishreen en octubre de 2019, el Gobierno bloqueó el acceso a internet durante más de 50 días. En ese período 23 civiles fueron asesinados a manos de las Fuerzas de Seguridad del Estado y grupos paramilitares como PMF[413]. Según Hayder Hamzoz, director del INSM Foundation for Digital Rights, durante los períodos de bloqueo de internet, la violencia de la policía y las milicias contra las defensoras de derechos humanos aumenta, al no poderse difundir de inmediato imágenes y vídeos de esos ataques[414]. También se realizaron apagones digitales durante el terremoto que afectó a Siria y el Norte de Irak, lo que provocó un impacto negativo en la distribución de la ayuda humanitaria[415]. Organizaciones internacionales y locales han iniciado diversas campañas contra estas prácticas entre las que destaca #KeepItOn[416].

Los bloqueos de internet fueron utilizados por primera vez en 2014 por las autoridades iraquíes para luchar contra el terrorismo del Estado Islámico. Desde entonces, como apunta el experto en derechos humanos Ismaeel Dawood, el Gobierno ha ido sofisticando esta estrategia incluyendo la coordinación con las autoridades de la Región del Kurdistán Iraquí (KRI) y las empresas proveedoras de servicios de telecomunicaciones y aplicaciones del país[417].

413 **Marwa Fatafta**. “From Free Space to a Tool of Oppression: What Happened to the Internet since the Arab Spring?,” The Tahrir Institute for Middle East Policy. 17 de diciembre de 2020. Disponible en: https://timep.org/2020/12/17/from-free-space-to-a-tool-of-oppression-what-happened-to-the-internet-since-the-arab-spring/

414 Hayder Hamzoz, entrevista personal por el equipo de investigación, 4 de junio de 2024.

415 **Dina Obaid**. “Social Media and Conflict in Irak. A Lexicon of Hate Speech Terms”. 2019. Disponible en: https://usercontent.one/wp/www.diraya.media/wp-content/uploads/2020/11/SOCIAL-MEDIA-AND-CONFLICT-IN-IRAQ.pdf

416 **Access Now.** *“Keep It On.”* Disponible en: https://www.accessnow.org/campaign/keepiton/

417 Ismaeel Dawood, entrevista persona por el equipo de investigación, 20 de junio de 2024.

3. EL CONTROL DE LOS CONTENIDOS DIGITALES: CENSURA Y VIGILANCIA MASIVA

El marco normativo que regula los cibercrímenes no solo es obsoleto, sino que es utilizado para limitar la libertad de expresión y el derecho a la no discriminación. Los delitos en los espacios digitales se regulan por la Ley Civil Nº 49 de 1951, la Ley de Comunicaciones de 2004 y el Código Penal Nº 11 de 1969[418]. Por ejemplo, el Código Penal iraquí, con provisiones utilizadas durante la ocupación británica, criminaliza contenidos digitales que supongan una "indecencia pública" (art. 401 y 403)[419] o que pretendan "cambiar los principios fundamentales de la constitución o las leyes básicas de la sociedad"[420]. Asimismo, el Gobierno del KRI dispone de la "Ley para prevenir el uso indebido de telecomunicaciones" para sancionar, incluso con penas de prisión, la difusión de amenazas, difamación, desinformación e injurias, entre otros, que atenten contra el honor o inciten a un delito moral[421]. En 2021, miembros de la organización kurda proderechos LGBTIQ+ Rasan, fueron arrestados por la policía por la difusión de contenido digital "contrario a la moral de la nación". Las autoridades apelaron al artículo 401 del Código Penal[422]. La represión contra Rasan, culminó en mayo de 2023, cuando un tribunal del KRI ordenó el cierre de la organización[423].

Para la implementación de este marco legal, existen dos mecanismos gubernamentales. Por un lado, la Comisión de Comunicaciones y Medios (CMC, por su acrónimo en inglés), creada en 2004, que realiza la vigilancia masiva y el control de los contenidos digitales de la sociedad civil, interactuando con las grandes empresas de telecomunicaciones de

418 **Aso Q. Abdullah, Sangar Y. Salih, and Jihad H. Mahmood.** *Invisible Threats: Digital Security and Female Journalists in Irak and the Kurdistan Region.* 2020.
Disponible en:
https://www.researchgate.net/publication/360024571_Invisible_Threats_Digital_Security_and_Female_Journalists_in_Iraq_and_the_Kurdistan_Region

419 El artículo 401 del código penal castiga a toda persona que cometa un "acto indecente" con penas de hasta seis meses de prisión o multa, o ambas penas. El artículo 403 del código estipula que toda persona que produzca o publique materiales que atenten contra la moral pública o la decencia con la intención de explotar o distribuir dichos materiales será castigada con penas de prisión de hasta dos años o multa, o ambas penas.

420 **Human Rights Watch**. *"'All This Terror because of a Photo'."* 2020.
Disponible en:
https://www.hrw.org/report/2023/02/21/all-terror-because-photo/digital-targeting-and-its-offline-consequences-lgbt

421 Ibid

422 Ibid

423 **Human Rights Watch**. *"Iraq." World Report 2024*.
Disponible en: https://www.hrw.org/world-report/2024/country-chapters/iraq

Irak[424]. Paralelamente, desde 2009, el Ministerio de Comunicaciones ha firmado varios contratos con empresas francesas para que suministren un sistema de monitoreo de internet y bloquear páginas webs[425], probablemente con las empresas francesas Safran y Thales[426]. También en ese periodo, el centro de investigación Citizen Lab, identificó aplicaciones de la Blue Coat Systems en las redes de telecomunicaciones de Bagdad vinculados con la red City Telecom, que permiten la vigilancia masiva[427].

Por otro lado, en enero de 2023, el Ministerio de Interior creó el Comité de Monitoreo de Contenido Digital para vigilar y censurar los contenidos digitales que son dañinos o contrarios a las normas sociales y culturales del país[428]. Con este fin, este comité lanzó ese mismo año la plataforma "Balgh" ("Informa", en inglés) para que la sociedad civil denuncie "contenidos de redes sociales que atentan contra la moral pública, contienen mensajes negativos e indecentes y socavan la estabilidad social" según palabras del ministro del Interior[429]. En tan solo un mes, se recibieron 96.000 denuncias de la sociedad civil[430], algunas de ellas continuaron en procesos legales en base al artículo 403 del Código Penal. Según Amnistía Internacional, ese mismo año el comité trasladó 16 casos a los tribunales penales[431]. Figuras públicas, modelos y artistas como Assal Houssam, Hassan Sajmah, Sayyed Ali, Saealusa y Umm Fahd han sido arrestadas y/o sancionadas por la publicación de contenido "indecente" a raíz de estos nuevos mecanismos[432]. Al menos 6 de ellas han sido

---

424 **Tech 4 Peace**. "Privacy in Irak -Case of Telecommunication Companies". 2023.
Disponible en:
https://t4p-storage.eu-central-1.linodeobjects.com/y778AhwIUwAvopYJsFmHZxsxStpSfb39zOnEXc0t.pdf

425 **OpenNet Initiative**. "Profiles: Iraq." Disponible en: https://opennet.net/research/profiles/iraq

426 **Tactical Report.** "Irak: Thales, Safran and Security Systems."
Disponible en: https://www.tacticalreport.com/daily/2635-Irak-thales-safran-and-security-systems

427 **Reporters Without Borders and the Citizen Lab.** *Planet Blue Coat: Mapping Global Censorship and Surveillance Tools*. 15 de noviembre de 2013.
Disponible en:
https://citizenlab.ca/2013/01/planet-blue-coat-mapping-global-censorship-and-surveillance-tools/

428 **Iraki News Agency**. Ministerio del Interior: formar un comité para monitorear el contenido en los sitios de redes sociales y responsabilizar a sus creadores. 16 de enero de 2023.
Disponible en:
https://www.ina.iq/175883--.html?__cf_chl_tk=wVv0deBsEkhWjoMlC5MepZzKdePd.PmTxkLzbeEojyg-1719559517-0.0.1.1-4543

429 **Safaa Ayyad**, "Irak's Controversial 'Ballegh' Platform for 'Combating Indecent Content,'" SMEX. 15 de febrero de 2023.
Disponible en: https://smex.org/iraqs-controversial-ballegh-platform-for-combating-indecent-content/

430 Hayder Hamzoz, entrevista personal realizada por el equipo de investigación, 4 de junio de 2024.

431 **Amnistía Internacional.** Iraq: Government must match rhetoric on human rights with meaningful action. 15 de marzo de 2023.
Disponible en:
https://www.amnesty.org/en/latest/news/2023/03/iraq-government-must-match-rhetoric-on-human-rights-with-meaningful-action/

432 **Ayad.** *"Irak's Controversial 'Ballegh' Platform for Combating Indecent Content."* 2023.
Disponible en: https://smex.org/iraqs-controversial-ballegh-platform-for-combating-indecent-content/.

sentenciadas a penas de cárcel en 2023[433] y al menos una de ellas ha sido asesinada[434].

Las actuales propuestas de ley para regular los espacios digitales apuntan incluso a mayores restricciones de la libertad de expresión en Irak. En la actualidad, el Gobierno iraquí discute un borrador de Ley de Cibercrimen que incluye penas de cárcel de hasta 10 años por publicar contenidos digitales que atenten contra los principios religiosos y sociales del país[435]. La Comisión de Comunicaciones y Medios (CMC) también está desarrollando la Regulación N°1 de 2023 sobre Contenido Digital para suprimir contenido online y sancionar delitos de las usuarias de internet[436]. Paralelamente, se discuten las leyes de Acceso a la Información y la Libertad de Expresión, ambas incluyen ambigüedades legales que podrían utilizarse para restringir libertades civiles[437]. Finalmente, el borrador de Ley de Reorganización de los Medios Electrónicos también ha levantado muchas críticas especialmente debido al potencial impacto negativo que puede tener sobre la libertad de expresión y libertad de prensa[438].

4. CAMPAÑAS DE ACOSO E INCITACIÓN AL ODIO CONTRA COLECTIVOS VULNERABILIZADOS

Las campañas de incitación al odio en las esferas digitales son también una constante en Irak. Líderes políticos, religiosos y militares promueven el discurso del odio para exacerbar las divisiones sectarias y ganar influencia política. En 2022, un clérigo y líder chiita pidió a la sociedad iraquí, a través de una publicación en la plataforma X (antigua Twitter),

433 **Amwaj.** "Cases against Social Media Influencers Raise Concerns over Freedoms in Irak". 10 de mayo de 2023. Disponible en: https://amwaj.media/article/Irak-influencers-social-media

434 **CBS News.** *Iraq investigating killing of social media influencer Um Fahad.* 2024. Disponible en: https://www.cbsnews.com/news/iraq-investigating-killing-um-fahad-social-media-influencer/

435 **Tech 4 Peace.** "Privacy in Irak. Case of Telecommunication Companies". 2023. Disponible en: https://t4p-storage.eu-central-1.linodeobjects.com/y778AhwIUwAvopYJsFmHZxsxStpSfb39zOnEXc0t.pdf

436 **Article 19.** "Irak: Drop draft Digital Content Legislation and Protect Free Speech Online". 16 de marzo de 2023. Disponible en: https://www.article19.org/resources/Irak-drop-draft-digital-content-legislation-protect-free-speech-online/

437 **Tech 4 Peace.** "Privacy in Irak -Case of Telecommunication Companies". 2023. Disponible en: https://t4p-storage.eu-central-1.linodeobjects.com/y778AhwIUwAvopYJsFmHZxsxStpSfb39zOnEXc0t.pdf

438 **Zhelwan Wali.** "Kurdish Parliament's Digital Media Regulation Bill Blurs Boundaries of Expression, Opponents Say". Rudaw.net. 2024. Disponible en: https://www.rudaw.net/english/kurdistan/17082020

luchar contra la comunidad LGBTIQ+, un acto que contribuyó a la intensificación del discurso de odio en las redes sociales[439]. En esta línea, el grupo de derechos humanos Iraqi Media House afirma que el "fenómeno de los ejércitos electrónicos ha alcanzado niveles peligrosos, emitiendo amenazas, incluida la incitación a la violencia y el odio"[440]. En esta línea, algunos casos[441] demuestran que mujeres candidatas políticas han sido objeto de extorsiones digitales[442], campañas de incitación al odio y amenazas con el objeto de que abandonaran sus carreras políticas[443]. Paralelamente, Naciones Unidas afirma que, desde 2016, al menos 36 defensoras de derechos humanos fueron asesinadas después de que hubieran sido acusadas por cuentas no autentificadas, bots y canales Telegram de ser agentes extranjeros o terroristas[444].

Las campañas de acoso online combinan prácticas de doxxing[445], publicación de datos personales y *fake news*[446] que ponen en serio peligro a las personas. Las mujeres se ven especialmente afectadas por la violencia digital[447]. Según la Misión de Naciones Unidas para Irak (UNAMI), campañas anónimas exponen públicamente a mujeres y niñas que han participado en manifestaciones contra el Gobierno, denunciando "conductas inmorales" a través de imágenes manipuladas[448]. Esta violencia digital provocó, durante las manifestaciones de octubre de 2019, que muchas mujeres dejaran de participar en las movilizaciones. Un caso especialmente relevante fue el asesinato en 2020 de la activista Reham Yacoub, después de una campaña de desinformación que la acusaba de tener vínculos

439 **Human Rights Watch.** *"'All This Terror because of a Photo'."* 2020.
Disponible en:
https://www.hrw.org/report/2023/02/21/all-terror-because-photo/digital-targeting-and-its-offline-consequences-lgbt

440 **The New Arab.** *Iran-backed 'electronic armies' threaten Iraqi activists, journalists.* 6 de septiembre de 2019.
Disponible en:
https://www.newarab.com/news/iran-backed-electronic-armies-threaten-iraqi-activists-journalists

441 **Tech4Peace.** "What Is the Truth about the News Attributed to the Journalist Noor Al-Jawaheri Regarding Her Being a Candidate and One of Her Priorities Is to Pass a Law Allowing the Men to Marry a Second Wife and with a Financial Grant of 25 Million Dinars to Encourage". 2021.
Disponible en: https://t4p.co/article/2021-07-21-the-journalist-nour-al-jawahiri

442 Ver glosario.

443 **Orto, N.** *Iraq elections: Why some female candidates refused to run.* The New Arab. 8 de octubre de 2021.
Disponible en: https://www.newarab.com/features/iraq-elections-why-some-female-candidates-refused-run

444 **Ali Al-Mikdam.** Fikra Forum. 2021.
Disponible en: https://www.washingtoninstitute.org/policy-analysis/ongoing-assassinations-iraqi-activists

445 Ver glosario.

446 Ver glosario.

447 **Abdelkarim Anwar, Assia; Ali Farhan, Walaa, & Aziz, Tara.** *Digital Violence against Women in Irak.* Octubre de 2023.
Disponible en: https://portal.salamatmena.org/wp-content/uploads/2024/01/Iraq-DVAW-2023-EN.pdf

448 **UNAMI, "Human Rights Violations and Abuses in the Context of Demonstrations in Irak".** 2020.
Disponible en:
https://www.ohchr.org/sites/default/files/Documents/Countries/IQ/Demonstrations-Iraq-UNAMI-OHCHR-report.pdf

con agentes norteamericanos[449].

El colectivo LGBTIQ+ es especialmente sensible a las campañas de acoso en línea por parte del Gobierno y milicias. Según Human Rights Watch, la vigilancia, acoso y amenazas online a personas LGBTIQ+ son una tendencia creciente en la región[450]. En abril de 2024, el Gobierno Federal Iraquí aprobó una ley que criminaliza y sanciona con penas de cárcel de hasta 15 años las relaciones sexuales homosexuales. En este marco se producen prácticas de entrampamiento[451] digital, en aplicaciones como Grindr, para forzar conductas inmorales, según la ley, de personas LGBTIQ+. A partir de estas prácticas, se producen arrestos arbitrarios, tortura y otros tratos degradantes e inhumanos[452]. Asimismo, las milicias también utilizan las redes sociales y aplicaciones de citas online para extorsionar digitalmente[453] [454] a las personas LGBTIQ+.

449 **Tech4Peace**, "From Invisibility to Visibility. Women's Digital Rights in Irak," Tech 4 Peace. 6 de marzo de 2023. Disponible en: https://t4p.co/blog/2023-03-06-from-invisibility-to-visibility-women-s-digital-rights-in-Irak

450 **Human Rights Watch.** *"'All This Terror because of a Photo'."* 2020. Disponible en: https://www.hrw.org/report/2023/02/21/all-terror-because-photo/digital-targeting-and-its-offline-consequences-lgbt

451 Ver glosario.

452 **Human Rights Watch.** *"'All This Terror because of a Photo'."* 2020. Disponible en: https://www.hrw.org/report/2023/02/21/all-terror-because-photo/digital-targeting-and-its-offline-consequences-lgbt

453 Ver glosario.

454 **Human Rights Watch.** *"'All This Terror because of a Photo'."* 2020. Disponible en: https://www.hrw.org/report/2023/02/21/all-terror-because-photo/digital-targeting-and-its-offline-consequences-lgbt

CONCLUSIONES

En general, se visibiliza una tendencia creciente en toda la región al autoritarismo y al control exhaustivo de la población, alentado por la aparición de nuevas herramientas tecnológicas, así como prácticas de infiltración online y suplantación de identidad cada vez más desacomplejadas y extendidas. Una tendencia agravada desde el inicio del genocidio en Gaza, en octubre de 2023, que, sin duda, deja intuir otra vuelta de tuerca más en la represión a las voces críticas no solo en el Maghreb y el Mashreq, sino también contra el activismo de los países occidentales que denuncia la inacción de la comunidad internacional o expresa su apoyo al pueblo palestino[1] [2].

En lo concreto, se identifican las siguientes tendencias:

1. MARCOS REGULADORES REPRESIVOS

El punto de partida de la vigilancia masiva en las regiones Maghreb y Mashreq son los entramados reguladores desarrollados para controlar a las disidencias políticas. Códigos penales con reminiscencias de los periodos coloniales se combinan con nuevas leyes para controlar las formas emergentes de activismo y comunicación social, bajo el pretexto de la seguridad nacional y la defensa de los valores morales del Estado. En este sentido observamos, por un lado, el uso de leyes y políticas antiterroristas para recortar derechos y ampliar los supuestos en los que se permite la vigilancia y la intercepción de comunicaciones de la población. En todos los casos, el terrorismo ha sido un fantasma convenientemente aprovechado para presentar a la disidencia política como una amenaza para la seguridad nacional. Y, en casos como Túnez, ha supuesto una excusa perfecta para limitar la movilidad y la circulación interna y hacia el extranjero de personas migrantes y de la disidencia política y de género.

Por otro lado, los regímenes autoritarios desarrollan nuevos instrumentos legales para controlar los contenidos y las nuevas formas de organización digital. Las leyes contra el cibercrimen que están siendo aprobadas en el Maghreb y Mashreq se justifican para prevenir conductas "inmorales", proteger a la infancia y prevenir la difusión de noticias falsas, entre otros. Sin embargo, la realidad es que han supuesto un punto de inflexión en el control de las comunicaciones digitales, lo que a su vez ha revertido en un aumento de la censura y la autocensura entre quienes se atreven a alzar sus voces críticas. Especial-

1 **Amnesty International.** *Europe: Authorities must protect the rights to freedom of expression and peaceful assembly ahead of Nakba Remembrance Day.* 10 de mayo de 2024.
Disponible en:
https://www.amnesty.org/en/latest/news/2024/05/europe-authorities-must-protect-expression-nakba/

2 **Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos.** (2024). *Global threats to freedom of expression arising from the conflict in Gaza.*
Recuperado de:
https://www.ohchr.org/es/documents/thematic-reports/a79319-global-threats-freedom-expression-arising-conflict-gaza-report

mente, desde ámbitos como el periodismo independiente, las organizaciones defensoras de derechos humanos y el colectivo LGBTIQ+. Lejos de evitar la circulación de información falsa, estas nuevas leyes están siendo utilizadas de forma generalizada en prácticamente todos los países analizados como herramienta para reducir al mínimo o suprimir la libertad de prensa y censurar el acceso a páginas web y medios de comunicación.

En este marco, se incluyen los casos de apagones digitales, que los gobiernos decretan especialmente en momentos de agitación social y protestas masivas, una táctica nada inocente tras la probada influencia que la Internet tuvo en la expansión del malestar que desembocó en las Primaveras Árabes. Estas estrategias obstruyen la capacidad de los movimientos sociales para organizarse y denunciar las vulneraciones de derechos humanos durante acontecimientos clave como las grandes movilizaciones. Irak es uno de los países que lidera esta estrategia política y digital, registrándose aumentos de la violencia policial y de las milicias en las protestas que se llevaron a cabo durante los bloqueos de internet.

2. ESTRATEGIAS Y TECNOLOGÍAS DE VIGILANCIA MASIVA

Las agencias de inteligencia de los gobiernos de Maghreb y Mashreq continúan utilizando la intercepción de comunicaciones como uno de los principales instrumentos para la vigilancia de periodistas, defensoras de derechos humanos y organizaciones de la sociedad civil. Sin embargo, esos mecanismos se han modernizado con la adquisición de tecnologías avanzadas como *spywares*[3] que penetran en los dispositivos móviles y ordenadores para sustraer información relevante de WhatsApp o fotografías.

La tecnología que hace posible la expansión de esta dinámica es proporcionada mayoritariamente por un pequeño grupo de empresas, entre las que se repiten algunas empresas occidentales como Hacking Team, Blue Coat y NSO Group. A través de estas empresas, Gobiernos como Israel, Marruecos o Líbano, entre otros, han desarrollado amplias campañas de vigilancia masiva para monitorear a defensoras de derechos humanos y acceder a su información personal y política.

Paralelamente, se identifica como nueva tendencia la introducción de la inteligencia artificial en armas no autónomas y drones para cuestiones que van desde extraer y almacenar información sensible de la población (por ejemplo, a través del reconocimiento facial[4]) a la programación de bombas en la ofensiva contra Gaza para aumentar su capacidad letal. Los drones son cada vez más utilizados para vigilar movilizaciones en países como Egipto, el Territorio Ocupado del Sáhara Occidental o en las calles de Jerusalén Este y Cisjordania, en Palestina.

3 Ver glosario.

4 Ver glosario.

3. ACOSO ONLINE

Los gobiernos de Maghreb y Mashreq son líderes globales en campañas de desinformación, en muchos casos dirigidos a atacar la reputación de organizaciones de la sociedad civil y de personas defensoras de los derechos humanos. Estos ataques online provienen de ejércitos electrónicos[5] formados por miles de bots, que apuntalan e intensifican el acoso cotidiano a las personas críticas y disidentes. Este tipo de campañas de acoso online llaman en ocasiones a la violencia física, aumentando el riesgo para la vida y la integridad de las personas defensoras. Se reportan en este informe diversos casos de agresiones físicas e incluso asesinatos precedidos por campañas de acoso online.

La Internet se ha convertido en un espacio tan útil y liberador como potencialmente peligroso para la sociedad civil, debido a las herramientas de monitoreo de los contenidos digitales en busca de posturas críticas con las acciones de los Gobiernos u otras fuerzas políticas en los países. Pero no solo las autoridades utilizan internet para rastrear y castigar los mensajes y publicaciones de las defensoras de derechos humanos, también otros actores -como sindicatos policiales, fuerzas parapoliciales o milicias- lideran, como en el caso de Egipto e Irak, estas acciones de rastreo y acoso.

En ocasiones, esta táctica incluso involucra al conjunto de la sociedad. Por ejemplo, en países como Irak y Marruecos, las autoridades han establecido plataformas para que la sociedad civil pueda reportar contenidos ofensivos o que ataquen la "moral" del país. En concreto, en el primer año de funcionamiento en Irak, se recogieron 96.000 denuncias.

4. IMPACTOS DIFERENCIALES

Estos impactos en términos de derechos no afectan a todas las personas de la misma manera, sino que intervienen variables como el género, la orientación sexual, la clase social y el estatus legal. Se percibe una tendencia creciente a exponer, acosar y vigilar a las mujeres que rompen con los estereotipos de género tradicionales y alzan sus voces para criticar la reducción del espacio democrático, la falta de derechos o la ocupación militar. Situación que deriva en su sometimiento a tipos de violencia específicos, como la violencia sexualizada, la exposición misógina en redes sociales, la publicación de información privada, como su contacto y dirección (el llamado "doxxing"), o los ataques al honor. Esas dinámicas específicas de coerción se ceban, también, con otros grupos vulnerabilizados como las personas LGBTIQ+, sometidas en buena parte de los países analizados al llamado "entrampamiento", es decir, a emboscadas a través de aplicaciones de contactos o bien en la calle para poder acusarlos de vulnerar los artículos legales que prohíben las

5 Ver glosario.

relaciones con personas del mismo sexo. También forma parte de esta dinámica la exposición no consentida de su orientación sexual, el llamado outing[6]; una práctica que puede elevar el riesgo a ser sometidas a más violencias.

La represión que aprovecha las desigualdades estructurales de género impacta, también, en algunos hombres. Es el caso de los periodistas marroquíes referenciados en el informe, que se vieron envueltos en procesos judiciales que utilizaban acusaciones muy graves, como los cargos de violación, para minar el potencial apoyo social que pueden recibir cuando son perseguidos por publicar reportajes y artículos críticos o incómodos para el poder.

La criminalización creciente de la migración y la deshumanización de las personas migrantes que atraviesan los países de la región en su camino hacia Europa (con una Unión Europea que deslocaliza el control de fronteras a estos países a cambio de paquetes económicos) tiene, también, su vertiente tecnológica. Además de ser objeto de acoso y difamación a través de medios digitales y redes sociales, las personas migrantes son el sujeto sobre el que se prueban tecnologías controvertidas como la biometría. En casos como el del Líbano, es habitual la incautación de móviles, ordenadores y otros medios de comunicación en campos de personas refugiadas sirias, acentuando el aislamiento social que ya sufren estas personas.

Por último, cabe destacar el impacto diferencial que la vigilancia masiva tiene sobre las poblaciones que viven bajo ocupación, como la palestina y la saharaui. Gran parte de las tecnologías identificadas se desarrollan y testean sobre el pueblo palestino que vive bajo ocupación militar israelí. Mientras que Marruecos se ha convertido en un actor fundamental para el desarrollo del sector en la región. El ecosistema empresarial se beneficia de la persistencia de estas ocupaciones y del genocidio contra el pueblo palestino.

Nada hace suponer que estas tendencias al aumento acelerado del control y la vigilancia sobre la población vayan a revertirse en los próximos años, sobre todo si se atiende a la creciente debilidad del sistema internacional de protección de los derechos humanos. Por ello, se hace imprescindible la generación de herramientas de análisis y autodefensa para las voces críticas y las personas defensoras de derechos humanos alrededor del mundo y, en este caso, en la franja sur de la región mediterránea. Con este informe, se pretende contribuir a este propósito: conocer el fenómeno, los impactos que genera en las personas defensoras de derechos humanos y visibilizar a las empresas implicadas. Este es el primer paso para construir alianzas de resistencia y colaboración, así como desarrollar estrategias de protección e incidencia política. Estrategias que también deben servir para establecer mecanismos de control para las empresas involucradas y exigir que los gobiernos garanticen los derechos humanos en el uso de las tecnologías.

6 Ver glosario.

RECOMENDACIONES

Las siguientes recomendaciones surgen de las principales conclusiones del presente informe, así como del análisis de las prácticas internacionales, estudios de casos y recomendaciones de diversas organizaciones de derechos humanos. El objetivo es proporcionar un marco integral para prevenir los riesgos de la vigilancia masiva y proteger la democracia y el espacio cívico.

Todas las recomendaciones aplican a todas las instituciones (gobiernos municipales y regionales, estados, Unión Europea y Naciones Unidas).

1. PROHIBICIÓN Y REGULACIÓN DE TECNOLOGÍAS INTRUSIVAS

- Moratoria sobre la exportación y uso de tecnologías de vigilancia: Los estados deben establecer de inmediato una moratoria sobre la venta, transferencia y uso de tecnología de vigilancia. Existe una necesidad urgente de detener las actividades llevadas a cabo mediante tecnologías de vigilancia de todos los estados y empresas, hasta que los marcos regulatorios aseguren el respeto de los derechos humanos.
- Prohibición total de la vigilancia masiva biométrica: Los estados deben prohibir el uso total, el desarrollo, la producción, la venta y la exportación de tecnologías de reconocimiento facial y otras formas de vigilancia biométrica sin excepciones.
- Prohibición de tecnologías probadas en contextos de conflicto o de ocupación: Los estados deben prohibir el uso, el desarrollo y la exportación de tecnologías de vigilancia probadas en conflictos armados o en contextos de ocupación de poblaciones civiles.
- Prohibición del uso de tecnologías de alto riesgo para los derechos fundamentales: Los estados deben prohibir en todos los casos el perfilado automatizado, el reconocimiento de emociones y la categorización biométrica en procedimientos de asilo y contextos migratorios y en cualquier tipo de proceso que pueda tener impacto sobre derechos fundamentales de las personas, como puede ser en el marco de una investigación policial.
- Prohibición del uso de software espía y protección de derechos: Los estados deben aprobar nuevos marcos jurídicos que aborden los desafíos que plantea el software espía, que incluyan una prohibición de la producción, exportación, venta, importación, adquisición, transferencia, mantenimiento y uso de software espía, ya que interfiere desproporcionadamente con los derechos fundamentales y para el cual no hay salvaguardias adecuadas para prevenir y reparar los daños a los derechos humanos.
- Garantizar programas de I+D libres de tecnología intrusiva: Las instituciones deben asegurar que los programas de I+D no colaboran con empresas vinculadas al desarro-

llo de tecnologías de vigilancia, incluidas las del ámbito militar.

2. TRANSPARENCIA Y RESPONSABILIDAD EN LA CONTRATACIÓN Y USO DE TECNOLOGÍAS DE VIGILANCIA

- Transparencia y auditoría de contratos públicos: Las instituciones deben asegurar la existencia e implementación mecanismos de control y auditoria de las contrataciones públicas de tecnología. Se deben incluir en la contratación pública evaluaciones de impacto sobre derechos fundamentales a cargo de la empresa prestadora del servicio con el fin de evitar afectaciones a derechos fundamentales antes de la puesta en marcha del servicio. En esa evaluación se deben incluir posibles medidas de mitigación e incluso de reparación para el caso de que haya afectaciones. Se podrían incluir mecanismos de reclamo ante las autoridades de contratación para que puedan recibir quejas de manera efectiva relacionadas a los efectos negativos sobre derechos humanos, vinculados o causados por la empresa prestataria del servicio.

- Transparencia y evaluación de riesgos: Las instituciones deben realizar evaluaciones de riesgo e impacto en derechos humanos antes de adquirir o implementar tecnologías de vigilancia, incorporando mecanismos de participación de la sociedad civil y grupos potencialmente afectados y otros actores con conocimiento técnico. Las empresas tecnológicas deben proporcionar transparencia sobre sus tecnologías, incluyendo información sobre la gestión de riesgos que realizan, información sobre los datos sobre los que se ha entrenado la tecnología -si incluye entrenamiento de datos- y las medidas de gobernanza de datos que han implementado para evitar sesgos. Deben también permitir auditorías de sus algoritmos, en un marco que garantice un suficiente nivel de confidencialidad.

- Responsabilidad y Transparencia en la Contratación Pública de Empresas Militares con fines vinculados a la Vigilancia: Las instituciones deben garantizar que el acceso de empresas militares a contrataciones públicas esté sujeto a estrictos estándares de derechos humanos, excluyendo a aquellas involucradas en violaciones graves. Deben promover el cumplimiento de normas internacionales como el Arreglo de Wassenaar y fomentar la transparencia en el comercio de tecnologías de vigilancia.

3. PROTECCIÓN DE LOS DERECHOS DIGITALES: PRIVACIDAD Y LA PROTECCIÓN DE DATOS

- Protección de datos personales y privacidad: Las instituciones deben garantizar que las tecnologías utilizadas respeten los derechos de privacidad y la protección de datos.
- Protección de la privacidad y ciberseguridad: Las legislaciones que regulen la privacidad electrónica deben incluir protecciones más estrictas para la confidencialidad de las comunicaciones y el derecho a la protección de los dispositivos conectados. Se debería mantener la seguridad de tales dispositivos durante toda su vida útil y establecer mecanismos de reclamación y reparación frente a riesgos de ciberseguridad.
- Sobre la vigilancia comercial: Las instituciones deben establecer una regulación clara que limite las prácticas de vigilancia comercial, protegiendo la privacidad de las consumidoras. Esto incluye la prohibición de la recopilación de datos sin el consentimiento explícito de las usuarias y la implementación de mecanismos de transparencia que permitan a las consumidoras conocer cómo se utilizan sus datos. Es necesario reforzar la legislación que establece salvaguardias para el acceso de las Fuerzas de Seguridad del Estado (FFSS) a los datos de empresas (e-evidence).

4. RENDICIÓN DE CUENTAS, PARTICIPACIÓN DE LA SOCIEDAD CIVIL Y ACCESO A LA JUSTICIA

- Fomento del debate público sobre vigilancia digital: Fomento del debate público sobre vigilancia digital: Las instituciones deben asegurar la participación de la sociedad civil de forma regular y significativa para debatir sobre el diseño y uso de tecnologías de vigilancia, así como su impacto en las libertades civiles y los derechos humanos.
- Rendición de cuentas y reparación: Las instituciones deben eliminar los obstáculos que impiden a las víctimas de vigilancia acceder a la justicia y garantizar investigaciones policiales y judiciales rápidas, efectivas y transparentes. Las víctimas deben tener acceso a la información intervenida y mecanismos de reparación. La sociedad civil debe participar en todo lo que tiene que ver con la utilización de tecnologías de vigilancia, de forma regular y relevante desde la fase de diseño, implementación, supervisión y control, así como también desde los procesos de contratación pública. Deben existir mecanismos de transparencia y acceso a información sobre estas tecnologías, como la existencia de registros públicos para que la población pueda

conocer dónde están implementadas estas tecnologías.

5. COOPERACIÓN Y ARMONIZACIÓN INTERNACIONAL

- Creación de un grupo de trabajo sobre vigilancia digital: Las instituciones deben establecer grupos de trabajo especializados para supervisar y analizar los abusos provocados por la vigilancia digital, desde lo local hasta nivel global, proponiendo recomendaciones para mitigar estos abusos.
- Extraterritorialidad en la legislación: Las instituciones deben incluir el principio de extraterritorialidad en todas las regulaciones en torno a la vigilancia masiva.
- Reformas legislativas y participación de la sociedad civil: Las instituciones deben reformar las leyes de seguridad para ajustarlas a los estándares de protección de derechos individuales y colectivos y garantizar la participación de la sociedad civil en los procesos legislativos.
- Obligaciones en materia de derechos humanos: La externalización de poderes de vigilancia a empresas privadas no exime a los estados y administraciones de sus obligaciones en materia de derechos humanos.
- Cumplimiento de los Principios Rectores sobre Empresas y Derechos Humanos del Consejo de Derechos Humanos: Las empresas deben operar de manera que respeten los derechos humanos en todas sus actividades, minimizando los riesgos de abuso. Los estados tienen que establecer regulaciones y políticas para asegurar que las empresas tecnológicas cumplan con estos principios de respeto, prevención y responsabilidad hacia los derechos humanos. Los estados deben incluir en sus marcos normativos mecanismos de reparación también en línea con los Principios Rectores.

6. REGULACIÓN Y SUPERVISIÓN DE LAS EMPRESAS QUE DESARROLLAN, INCORPORAN Y UTILIZAN TECNOLOGÍA DE VIGILANCIA

- Responsabilidad y diligencia debida en derechos humanos: Las empresas de vigilancia y de aquellas que recopilan datos de forma masiva, deben integrar la diligencia

debida en materia de derechos humanos en todas las etapas del desarrollo de sus productos y mantener involucrada a la sociedad civil de forma significativa.

- Auditorías y transparencia: Las empresas deben realizar auditorías anuales externas para evaluar el impacto de sus productos sobre los derechos humanos y facilitar el acceso para supervisar riesgos sistémicos.
- Inversiones respetuosas con los derechos humanos: Se insta a las personas y entidades inversoras a adoptar principios de inversión ética que prioricen el respeto a los derechos humanos en sus decisiones.

7. REFUERZO DE LA SOBERANÍA TECNOLÓGICA

- Interoperabilidad y alternativas: Los estados deben garantizar que las personas puedan elegir alternativas respetuosas con los derechos frente a las plataformas tecnológicas dominantes, exigiendo interoperabilidad entre estas plataformas.
- Normas de contratación pública: Los estados deben establecer criterios que prioricen la transparencia y la ética en la selección de proveedores que cumplan con los estándares de derechos humanos.
- Código Abierto: Los estados deben fomentar el uso de software de código abierto para garantizar la auditoría y el acceso público a las herramientas utilizadas en la recopilación y análisis de datos, promoviendo la transparencia y la confianza.
- Financiación pública: Los estados deben dedicar fondos públicos a iniciativas que se centren en la recopilación ética de datos, priorizando proyectos que protejan la privacidad de los usuarios y promuevan el uso responsable de la tecnología.

ANEXOS

1. GLOSARIO

- **Amenazas Persistentes Avanzadas (APT):** técnicas sistemáticas de hackeo para acceder a un sistema digital y permanece en él durante un periodo prolongado con fines maliciosos como sustracción de datos personales.
- **Ataque DDoS:** Un ataque DDoS (Distributed Denial of Service) es un tipo de ciberataque que busca interrumpir el funcionamiento de un sitio web o servicio en línea. Esto se logra al sobrecargar el servidor con una gran cantidad de solicitudes de acceso simultáneas, enviadas desde múltiples dispositivos o "bots" infectados. Esta afluencia masiva de tráfico puede ralentizar el sitio o incluso hacer que deje de funcionar temporalmente, impidiendo el acceso a usuarios legítimos.
- **Ataques zero-click o inyecciones en red:** técnicas de *spyware* que permiten infiltrar un dispositivo sin necesidad de interacción por parte del usuario afectado.
- **Comportamiento Inauténtico Coordinado *(Astroturfing)*:** enmascaramiento de la organización y dirección de una campaña coordinada para que parezca que surge espontáneamente de la población y de la sociedad civil.
- **Data breach:** acceso y robo de información sensible o confidencial por medios ilícitos o ilegales.
- **Inspección Profunda de Paquetes (DPI - Deep Packet Inspection):** un tipo de procesamiento de datos usado para muchas funciones, entre ellas el control, filtrado y bloqueo de la actividad en Internet a tiempo real y de manera dirigida.
- **Doxxing:** publicar información personal y documentos audiovisuales de una persona sin su consentimiento.
- **Ejército Electrónico:** grupo de hackers que apoya las acciones de un determinado Gobierno y cuya misión es utilizar Internet, redes sociales y ataques cibernéticos para luchar contra los adversarios políticos.
- **Emboscada o entrampamiento digital:** engañar a alguien para que cometa un crimen (según las leyes del país) en los espacios digitales.
- **Extorsión digital o cibernética:** es una forma de delito informático en la que individuos chantajean digitalmente a organizaciones o personas para obtener lo que quieren. Pueden amenazar con filtrar datos, lanzar ataques cibernéticos, deshabilitar operaciones, evitar que los usuarios accedan a los datos o incluso llegar a destruir los datos obtenidos.
- ***Fake news:*** se usa para referirse a la difusión de noticias falsas o bulos, con el objetivo de crear un estado de opinión particular, confundir y desinformar a la audiencia.

- **Granja o fábrica de trolls (o *trolling online*)**: Pueden ser un grupo de cuentas automáticas (bots) o personas pagadas para influenciar la opinión pública a través de las redes sociales en temas políticos o de actualidad.
- ***Malware:*** cualquier tipo de programa o código diseñado con diseñado para dañar, explotar o infiltrarse en sistemas informáticos sin el consentimiento de la usuaria.
- ***OAuth Phishing (Open Authorisation Phishing):*** modalidad del *phishing* en la que se engaña a los usuarios para que otorguen permisos a aplicaciones maliciosas que pueden acceder a los datos de su cuenta y realizar acciones en su nombre.
- ***Outing:*** hacer pública la identidad sexual o de género de una persona sin su consentimiento.
- ***Phishing:*** esta técnica informática consiste en hacerse pasar por una persona, empresa o servicio de confianza para engañar a una víctima, ganándose su confianza para estafarla o vigilar sus comunicaciones.
- **Reconocimiento facial:** identificación biométrica de la identidad de una persona a partir de ciertos puntos físicos de la cara.
- ***Spyware:*** un tipo de *malware* que, aunque puede no dañar el ordenador, controla y espía a escondidas todas las acciones que se realizan a través del ordenador infectado.
- ***Trojan Horse* o virus troyano:** un tipo de *malware* que se esconde tras otro archivo aparentemente inocuo para ganar acceso a algún sistema sin ser detectado. Hay muchos tipos de troyanos (un ejemplo es el backdoor trojan, que abre acceso para proporcionar el control remoto de un ordenador).

2. DIRECTORIO
de empresas de vigilancia masiva operando en el Maghreb y Mashreq

- **AGT (Advanced German Technologies)**: empresa con sede en Dubai. Se dedica principalmente a la reventa de equipos forenses digitales y servicios de tecnología de vigilancia. Su tecnología ha sido utilizada en **Siria**[1].
- **Amesys (Advanced Middle East Systems):** empresa francesa bajo el control de la también francesa Bull. Amesys desarrolló el sistema Eagle System de vigilancia digital masiva de tráfico con funciones de censura (a través de Deep Packet Inspection). En 2015 Amesys pasa a llamarse Nexa Technologies y crea un nuevo sistema de vigilancia masiva con el nombre de "Cerebro", con la capacidad de rastrear telecomunicaciones a tiempo real. Ha sido utilizada en **Marruecos**[2] y **Egipto**[3].
- **Anyvision:** empresa israelí especializada en reconocimiento facial a través de cámaras inteligentes. La tecnología de esta empresa se utiliza en puntos de control militar israelí contra la población en **Palestina**[4].
- **AREA SpA:** empresa italiana que en colaboración con Utimaco y Qosmos ha participado en el desarrollo de un sistema central de monitoreo utilizado para el control y la vigilancia de la población **siria**[5] liderado por Syrian Telecom.

---

1 **Franceschi-Bicchierai, Lorenzo.** "European Surveillance Companies AGT and RCS Sell Syria Tools of Oppression." Vice. 12 de diciembre de 2016.
Disponible en:
https://www.vice.com/en/article/european-surveillance-companies-agt-rcs-sell-syria-tools-of-oppression/.

2 **Reflets.info.** "Maroc : Popcorn, le projet qui n'existait pas," 15 de noviembre de 2017.
Disponible en: https://reflets.info/articles/maroc-popcorn-le-projet-qui-n-existait-pas.

3 **Tesquet, Olivier.** "Amesys: Egyptian Trials and Tribulations of a French Digital Arms Dealer." Télérama, 5 de julio de 2017.
Disponible en:
https://www.telerama.fr/monde/amesys-egyptian-trials-and-tribulations-of-a-french-digital-arms-dealer,160452.php

4 **"Who Profits: Company Profile."** Who Profits.
Disponible en: https://www.whoprofits.org/companies/company/6872/ar.

5 **Franceschi-Bicchierai, Lorenzo.** "Italian Cops Raid Surveillance Tech Company Area Spa Selling Spy Gear to Syria." Vice, 1 de diciembre de 2016.
Disponible en:
https://www.vice.com/en/article/italian-cops-raid-surveillance-tech-company-area-spa-selling-spy-gear-to-syria

- **Baykar:** empresa turca creada en 1984 y especializada en la producción de drones de vigilancia y reconocimiento. Los drones Bayraktar TB2 han sido utilizados en los conflictos de Libia, **Siria** y Nagorno-Karabag. En 2021, **Marruecos** ha utilizado sus drones para actividades de reconocimiento en el **Sáhara Occidental**[6].

- **Blue Bird Aero Systems:** empresa israelí especializada en el diseño y producción de drones desde 2002. Israel Aerospace Industries posee el 50% de sus acciones. Actualmente hay una planta de producción de los drones tipo WanderB y ThunderB especializados en misiones de reconocimiento y vigilancia en **Marruecos**[7].

- **Blue Coat Systems:** empresa norteamericana adquirida en 2016 por Symantec. Posteriormente Symantec fue absorbida por la empresa californiana Broadcom en 2019. La marca Blue Coat desaparece desde entonces, pero sus sistemas siguen siendo utilizados por Broadcom. Su tecnología sirvió para interceptar e inspeccionar datos de las redes de telecomunicaciones para la vigilancia masiva de dispositivos móviles, ordenadores, interacciones en las redes sociales, correos electrónicos y comunicaciones online. Estos sistemas fueron adquiridos y utilizados por los Gobiernos de **Irak**[8], **Líbano**[9], **Siria**[10] y **Túnez**[11].

6 **Soriano, Ginés.** " Marruecos comienza a recibir Drones de combate fabricados en Turquía." InfoDefensa, 23 de septiembre de 2021.
Disponible en:
https://www.infodefensa.com/texto-diario/mostrar/3206127/marruecos-comienza-recibir-drones-combate-fabricados-turquia.

7 **Aublanc, Alexandre.** "Morocco to Become Rare Military Drone Manufacturer Thanks to Cooperation with Israel." Le Monde. 9 de mayo de 2024.
Disponible en:
https://www.lemonde.fr/en/le-monde-africa/article/2024/05/09/morocco-to-become-rare-military-drone-manufacturer-thanks-to-cooperation-with-israel_6670920_124.html.

8 Citizen Lab. "Planet Blue Coat: Mapping Global Censorship and Surveillance Tools." January 2013.
https://citizenlab.ca/2013/01/planet-blue-coat-mapping-global-censorship-and-surveillance-tools/.

9 **Marquis-Boire et al.** "Appendix A: Summary Analysis of Blue Coat: Countries of Interest". The Citizen Lab. 15 enero de 2013.
Disponible en:
https://citizenlab.ca/2013/01/appendix-a-summary-analysis-of-blue-coat-countries-of-interest/

10 **The Citizen Lab.** "Behind Blue Coat." 2011.
Disponible en: https://citizenlab.ca/2011/11/behind-blue-coat/

11 **Goupy, Marie.** «La bienveillante neutralité des technologies d'espionnage des communications: le cas tunisien.» Cultures & conflits, n.° 93. 8 de julio de 2014.
Disponible en: https://journals.openedition.org/conflits/18863

- **Circles:** empresa de ciber-vigilancia israelí creada en 2011. Tanto NSO Group como Circles están bajo el control de la empresa de capital de inversión tecnológica norteamericana Francisco Partners. Su tecnología se especializa en identificar vulnerabilidades en las redes de comunicación para interceptar llamadas, textos, monitorear localizaciones de dispositivos móviles, entre otros. **Israel** y **Marruecos**[12] habrían utilizado esta tecnología.

- **Cognyte:** empresa israelí especializada en soluciones de ciberseguridad. Su tecnología de investigación se utiliza para identificar amenazas de seguridad en las esferas analíticas. Sin embargo, su software ha sido utilizado en **Marruecos**[13] [14] para la creación y gestión de cuentas falsas en redes sociales como Facebook, Instagram, Twitter, YouTube o VKontakte.

- **Corsight AI:** empresa israelí especializada en reconocimiento facial. La canadiense Awz es propietaria de esta empresa. Los servicios de inteligencia israelíes, así como la Unidad 8200 utilizan esta tecnología para vigilar a la población **palestina**[15].

- **Cytrox:** compañía creada en 2017 y con sede oficial en Macedonia del Norte, pero operada desde Hungría e Israel, célebre por su *malware* usado para ciberataques y vigilancia encubierta. Cytrox forma parte de Intellexa Consortium, un grupo de empresas de *spyware*. Su producto Cytrox Predator ha sido utilizado en **Egipto**[16] contra opositores políticos y periodistas.

- **Dahua Technologies:** empresa con sede en Hangzhou, China, especializada en el diseño y producción de tecnologías de vigilancia y seguridad. Sus cámaras de lectura de matrículas de vehículo, reconocimiento facial y detección de movimiento se encuentran en el **Territorio Ocupado de Palestina**[17].

---

12 **Citizen Lab.** "Running in Circles: Uncovering the Clients of Cyberespionage Firm Circles." 1 de diciembre de 2020. Disponible en: https://citizenlab.ca/2020/12/running-in-circles-uncovering-the-clients-of-cyberespionage-firm-circles/

13 **DFRLab.** "Mythical Beasts and Where to Find Them: Report," DFRLab. 4 de septiembre de 2024. Disponible en: https://dfrlab.org/2024/09/04/mythical-beasts-and-where-to-find-them-report/.

14 45 Mike Dvilyanski, David Agranovich y Nathaniel Gleicher. "Threat Report on the Surveillance-for-Hire Industry," Meta, 16 de diciembre de 2021. Disponible en: https://about.fb.com/wp-content/uploads/2021/12/Threat-Report-on-the-Surveillance-for-Hire-Industry.pdf.

15 **Frenkel, Sheera.** "Israel Uses Facial Recognition in Gaza," The New York Times. 27 de marzo de 2024. Disponible en: https://www.nytimes.com/2024/03/27/technology/israel-facial-recognition-gaza.html.

16 **Citizen Lab.** "Predator in the Wires: Ahmed Eltantawy Targeted with Predator Spyware After Announcing Presidential Ambitions," 20 de septiembre de 2023. Disponible en: https://citizenlab.ca/2023/09/predator-in-the-wires-ahmed-eltantawy-targeted-with-predator-spyware-after-announcing-presidential-ambitions/

17 **Who Profits.** "Surveillance: The Global Industry Behind the Technology of Control," Who Profits. Noviembre de 2018. Disponible en: https://www.whoprofits.org/writable/uploads/old/uploads/2018/11/surveil-final.pdf

- **ETI:** empresa danesa especializada en ciberseguridad y cibervigilancia que en 2011 fue adquirida por la multinacional alemana BAE Systems. ETI desarrolló el software Evident y X-Stream para rastrear los hábitos de navegación de las usuarias de internet, desencriptar e interceptar llamadas y correos electrónicos. **Marruecos**[18] ha adquirido esta tecnología. En **Túnez**[19] además se identifica el uso de esta tecnología para reprimir opositores durante el régimen de Ben-Ali.

- **Gamma Group:** empresa británica especializada en ciberseguridad y el desarrollo de soluciones tecnológicas de vigilancia. Uno de sus principales productos es el *spyware* FinFisher o FinSpy que puede ser usado para la infección de ordenadores y dispositivos móviles con el fin de realizar sustracción de datos. La tecnología FinFisher fue encontrada en una sofisticada infraestructura de ciberespionaje, conocida como Dark Caracal, vinculada a los servicios de inteligencia del **Líbano**[20]. **Egipto**[21] y **Marruecos**[22] también adquirieron esta tecnología para la interceptación de telecomunicaciones.

- **Guardia Systems:** empresa libanesa, que forma parte del MG Holding group. Guardia está especializada en el desarrollo de soluciones tecnológicas en el sector de la ciberseguridad para empresas extractivistas, Gobiernos e infraestructuras críticas. Ha instalado sistemas de cámaras de videovigilancia en Beirut, **Líbano**[23] en 2016 con capacidad de lectura y registro de matrículas de vehículos, así como en sistemas de vigilancia en **Irak**[24].

---

18 **BBC News.** "Israel to Set Up New Military Unit to Combat Hamas Cyber Threats," 21 de junio de 2017. Disponible en: https://www.bbc.com/news/world-middle-east-40276568

19 Ibid.

20 **The Hacker News.** "Researchers Uncover Government-Sponsored Mobile Hacking Group Operating Since 2012." 19 de enero de 2018.
Disponible en: https://thehackernews.com/2018/01/dark-caracal-android-malware.html.

21 **Amnesty International.** "German-Made FinSpy Spyware Found in Egypt, and Mac and Linux Versions Revealed," Amnesty International, 25 de septiembre de 2020.
Disponible en:
https://www.amnesty.org/en/latest/research/2020/09/german-made-finspy-spyware-found-in-egypt-and-mac-and-linux-versions-revealed/

22 **Charlie Osborne**, "In Hacking Team's wake, FinFisher spyware rises in popularity with government users," *ZDNet*, 19 de octubre de 2015.
Disponible en:
https://www.zdnet.com/article/in-hacking-teams-wake-finfisher-spyware-rises-in-popularity-with-government-users/.

23 **Inavate.** "Beirut Surveillance Project Protects the City." 2024.
Disponible en: https://www.inavateonthenet.net/case-studies/article/beirut-surveillance-project-protects-the-city.

24 **Intelligence Online.** "Lebanese Entrepreneur Ziad Monla Vies to Fill Iraqi Defence's Critical Communications Needs." Intelligence Online. 6 de octubre de 2023.
Disponible en:
https://www.intelligenceonline.com/international-dealmaking/2023/10/06/lebanese-entrepreneur-ziad-monla-vies-to-fill-iraqi-defence-s-critical-communications-needs,110062357-gra.

- **Hacking Team (HT):** empresa italiana ya desaparecida conocida por el desarrollo del software de vigilancia masiva Remote Control System. Este *spyware* permitía la captura de datos de móviles y comunicaciones en plataformas como Skype, así como el monitoreo de localización por GPS de los dispositivos. Su tecnología fue adquirida por los servicios de inteligencia de **Marruecos**[25] y **Líbano**[26], y que ha servido para perseguir a defensoras de derechos humanos y periodistas.

- **Hikvision:** empresa multinacional china líder en soluciones de videovigilancia. Las cámaras de detección de movimiento y reconocimiento biométrico se encuentran en **Túnez**[27] y en **Jerusalén**[28].

- **Idemia:** multinacional francesa especializada en sistemas de identificación biométrica automatizada. Anteriormente llamada Morpho, forma parte de Advent International desde 2017, un fondo de capital privado. Su producto MBIS, que permite obtener huellas dactilares, huellas de la palma y rasgos faciales, ha sido vendido recientemente al Gobierno de **Túnez**[29] para reforzar la seguridad de las fronteras.

- **Indra Sistemas:** empresa española con participación pública, especializada en soluciones tecnológicas para el sector de defensa y ciberseguridad a nivel global y con participación pública entre sus accionistas. En 2019, contribuyó en la expansión de la red de vigilancia por satélite para el control del espacio aéreo del sur de **Marruecos** y el **Sáhara Occidental**[30], mediante la instalación de sistemas avanzados de comunicaciones y vigilancia.

---

25 **Citizen Lab.** "Backdoors Are Forever: Hacking Team and the Targeting of Dissent," Citizen Lab, 7 de octubre de 2012.
Disponible en:
https://citizenlab.ca/2012/10/backdoors-are-forever-hacking-team-and-the-targeting-of-dissent/

26 **SMEX.** "HackingTeam Leaks: Lebanon's Cybercrime Bureau Exploited Angry Birds to Surveil Citizens' Mobile Devices". 30 de julio de 2015.
Disponible en:
https://smex.org/hackingteam-leaks-lebanons-cybercrime-bureau-exploited-angry-birds-to-surveil-citizens-mobile-devices/

27 **Hikvision.** "Safe City Solutions." Disponible en: https://hikvision.az/en/solution/safe-city/

28 **Amnesty International.** "Israeli Authorities Are Using Facial Recognition Technology to Entrench Apartheid," 24 de mayo de 2023.
Disponible en:
https://www.amnesty.org/en/latest/news/2023/05/israel-opt-israeli-authorities-are-using-facial-recognition-technology-to-entrench-apartheid/

29 **Actu-Maroc**, "Kaïs Saied lance un programme de sécurité numérique en Tunisie malgré la crise économique,". 1 de marzo de 2024.
Disponible en:
https://www.actu-maroc.com/kais-saied-lance-un-programme-de-securite-numerique-en-tunisie-malgre-la-crise-economique/.

30 **Indra Sistemas, S.A.** "Indra Sistemas, S.A." ODHE.
Disponible en: https://www.odhe.cat/es/indra-sistemas-s-a/.

- **Inmobiles:** empresa libanesa, subsidiaria de la británica Resource Holding Group, que aporta sistemas de captura biométrica para registrar usuarios que compran dispositivos móviles en el **Líbano** de acuerdo con el registro de móviles (International Mobile Equipment Identity - IMEI)[31].
- **IrisGuard:** empresa británica fundada en 2011 y especializada en soluciones biométricas. Varios fondos de inversión como GrowthGate Capital se encuentran entre sus propietarios. Sus sistemas de identificación biométrica son utilizados para registrar a las refugiadas sirias que solicitan ayudan a las agencias de Naciones Unidas en **Jordania**[32].
- **Magal Security Systems:** empresa israelí líder global de sistemas perimetrales. Creada en 1969 a partir de la empresa pública Israeli Aerospace Industries (IAI). Desde entonces ha aportado sistemas de vallado inteligente con sensores de detección de movimiento y cámaras de videovigilancia modernas para los asentamientos ilegales y el Muro de Apartheid de **Israel** en **Palestina**[33].
- **Mer Group:** empresa israelí especializada en sistemas de vigilancia masiva. Su tecnología se encuentra en el proyecto Mabat 2000 para la vigilancia de la ciudad vieja de **Jerusalén** y el control de la población **palestina**[34].
- **MSAB (Mycro Systemation AB):** empresa tecnológica de nacionalidad sueca, líder mundial en extracción y análisis de datos de móviles. La empresa franco-libanesa Intertech suministró a **Marruecos** esta tecnología. **Marruecos**[35] podría haber utilizado esta tecnología para perseguir a la disidencia política y defensoras de derechos humanos al no existir controles sobre el uso de esta tecnología (que fue transferida por la UE para el control de fronteras).

31 **SMEX.** "Ministry of Telecommunications IMEI Registration Policy Threatens Digital Privacy," 4 de diciembre de 2018.
Disponible en:
https://smex.org/ministry-of-telecommunications-imei-registration-policy-threatens-digital-privacy/.

32 **Access Now.** "IrisGuard's Biometric Technology Leaves Refugees in Jordan Vulnerable," 12 de abril de 2021.
Disponible en: https://www.accessnow.org/press-release/irisguard-refugees-jordan/

33 **Daza, Felip.** "Los Muros Globalizados de la Ocupación. La trazabilidad de los productos de Magal Security Systems en las cadenas de suministro de la ciberseguridad en Israel y Palestina". Barcelona. ODHE y Shock Monitor. 2020.
Disponible en: https://novact.org/wp-content/uploads/2023/10/Informe_Muros-invisibles_ocupacion.pdf

34 **Who Profits.** "Mer Industries,".
Disponible en: https://www.whoprofits.org/companies/company/4041?c-mer-industries.

35 **Disclose.** "How the EU Supplied Morocco with Phone Hacking Spyware," Disclose, 25 de julio de 2022.
Disponible en:
https://disclose.ngo/en/article/how-the-eu-supplied-morocco-with-phone-hacking-spyware.

- **MTN Syria:** proveedor de servicios móviles, subsidiaria de la empresa sudafricana MTN. MTN ha dado apoyo al Gobierno **sirio**[36] en lo que respecta al filtrado y bloqueo de las telecomunicaciones de sus usuarios.

- **NSO Group:** empresa israelí con sede en Herzliya, especializada en el desarrollo de *spywares* para monitorear e interceptar datos de dispositivos móviles. Su producto más conocido, el *spyware* Pegasus, es capaz de sustraer datos de correos electrónicos, llamadas, imágenes y activar la cámara de los móviles incluso sin necesidad de interacción por parte del usuario afectado. Pegasus ha sido adquirido por **Marruecos, Líbano, Jordania** e **Israel** y ha sido usado para espiar a líderes políticas, periodistas y defensoras de derechos humanos. Las autoridades marroquíes e israelíes también han utilizado el *spyware* Pegasus para vigilar y controlar la población civil **palestina** y **saharaui**[37].

- **Oxygen Forensics:** empresa especializada en informática forense con sede en Virginia, Estados Unidos. Uno de sus principales productos tecnológicos es el Oxygen Forensic Detective que tiene capacidad de análisis y extracción de datos de móviles. Las autoridades marroquíes accedieron a esta tecnología en 2022 a través de la empresa franco-libanesa Intertech. **Marruecos**[38] podría haber utilizado esta tecnología para perseguir la disidencia política y defensoras de derechos humanos al no existir controles sobre el uso de esta tecnología (que fue transferida por la UE para el control de fronteras).

- **Palantir Technologies:** empresa creada en 2003 con sede en Denver, Estados Unidos, se especializa en análisis de datos y softwares con IA. Su tecnología es utilizada por el ejército israelí para sus operaciones militares en **Palestina**[39].

- **Qosmos:** compañía francesa que suministró al STE (Establecimiento de Telecomunicaciones de **Siria**[40]) herramientas de inspección profunda de paquetes (DPI), finalizando el proyecto en 2012.

---

36 **Digital Dominion Report.** 2021.
Disponible en: https://media.business-humanrights.org/media/documents/Digital-dominion-Syria-report.pdf

37 **Ronen Bergman.** "The NSO Group's Israeli Spyware and the Global Surveillance Industry," The New York Times, 28 de enero de 2022.
Disponible en: https://www.nytimes.com/2022/01/28/magazine/nso-group-israel-spyware.html.

38 **Disclose.** "How the EU Supplied Morocco with Phone Hacking Spyware," Disclose, 25 de julio de 2022.
Disponible en:
https://disclose.ngo/en/article/how-the-eu-supplied-morocco-with-phone-hacking-spyware.

39 **American Friends Service Committee.** "Palantir Technologies".
Disponible en: https://investigate.afsc.org/company/palantir-technologies

40 **European Center for Constitutional and Human Rights (ECCHR).** "Surveillance in Syria: European Firms May Be Aiding and Abetting Crimes Against Humanity,"
Disponible en:
https://www.ecchr.eu/en/case/surveillance-in-syria-european-firms-may-be-aiding-and-abetting-crimes-against-humanity/

- **Grupo Safran:** multinacional francesa creada en 2005 por empresas del sector de defensa. Safran participó, junto con otras empresas como Motorola, Northrup Grumman o L-1, en el desarrollo del Sistema automatizado de identificación biométrica (ABIS) para el registro y sistematización de datos biométricos de la población de **Irak** y **Afganistán**[41]. En 2009 el Ministerio de Comunicaciones de **Irak**[42] contrató a Safran para desarrollar un sistema de monitoreo de internet y bloqueo de páginas web.

- **Sandvine:** empresa canadiense especializada en la inspección profunda de paquetes (DPI). En el caso de **Egipto**[43], esta tecnología ha sido usada para cerrar más de 600 medios críticos o webs de organizaciones de defensa de los derechos humanos, lo que le ha valido entrar en un listado del Departamento del Tesoro de Estados Unidos.

- **Thales Group:** multinacional francesa del sector aeroespacial, defensa, seguridad e identidad digital, creada en 1893 y con participación del Gobierno francés. De forma directa o a través de su subsidiara Gemalto, ha aportado tecnología que ha sido usada para la captura de datos biométricos en documentos de identificación en el **Líbano**[44] y **Marruecos**[45]. También se identifican contratos con el Ministerio de Comunicaciones de **Irak**[46] sobre sistemas de vigilancia.

- **TKH Group:** empresa tecnológica con sede en los Países Bajos que se especializa en el desarrollo de sistemas de vigilancia, comunicaciones y conectividad. Su subsidiaria TKH Security Solutions, vende cámaras de vigilancia, bajo su propio nombre y la marca Grundig a la policía **israelí** y a los asentamientos ilegales israelíes. A partir de 2023, se han instalado varias cámaras de circuito cerrado de televisión de TKH Security y Grundig en la vigilancia policial y otras infraestructuras de las zonas residenciales de **Jerusalén Este**[47].

---

41 **Nina Toft Djanegara.** "Biometrics for Counter-Terrorism: Case Study of the U.S. Military in Iraq and Afghanistan," Privacy International. Junio 2021.
Disponible en:
https://privacyinternational.org/sites/default/files/2021-06/Biometrics%20for%20Counter-Terrorism-%20Case%20study%20of%20the%20U.S.%20military%20in%20Iraq%20and%20Afghanistan%20-%20Nina%20Toft%20Djanegara%20-%20v6.pdf

42 **Tactical Report.** "Irak: Thales, Safran and Security Systems."
Disponible en: https://www.tacticalreport.com/daily/2635-Irak-thales-safran-and-security-systems

43 **Peter Guest.** "U.S. Sanctions Sandvine Over Egypt's Internet Censorship," Wired, 28 de febrero de 2024.
Disponible en: https://www.wired.com/story/sandvine-us-sanctions-egypt-internet-censorship/

44 **Thales Group.** "Lebanese Passport."
https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/customer-cases/lebanese-passport.

45 **Thales Group.** "Thales in Morocco," Thales Group.
Disponible en: https://www.thalesgroup.com/en/countries/middle-east-and-africa/thales-morocco

46 **Tactical Report.** "Irak: Thales, Safran and Security Systems."
Disponible en: https://www.tacticalreport.com/daily/2635-Irak-thales-safran-and-security-systems

47 **American Friends Service Committee.** "TKH".
Disponible en: https://investigate.afsc.org/company/tkh.

- **Total Secure Defence (TSA):** empresa con sede en los Emiratos Árabes Unidos y proveedora de sistemas y equipamiento de seguridad. En **Marruecos**[48] se han adquirido sus productos tales como sistemas de vigilancia y *IMSI Catchers* (dispositivos que engañan a los dispositivos móviles para obtener toda la información relacionada con el teléfono) usados sobre la interceptación de datos de telecomunicaciones en tiempo real.

- **Trovicor:** inicialmente creada como un departamento de inteligencia de Siemens. A partir de 2009, es adquirida por un fondo de inversión y se constituye como empresa con sede en Dubai. A partir de 2019 es adquirida por la francesa Boss Industries. Trovicor se especializa en servicios de inteligencia y ciberseguridad. El régimen de Ben-Ali adquirió sus sistemas de interceptación, análisis de datos de telecomunicaciones y rastreo de localizaciones de dispositivos móviles de la sociedad civil de **Túnez**[49].

- **Utimaco:** empresa de ciberseguridad con sede en Alemania y Estados Unidos. En 2021 fue adquirida por el fondo SGT Capital. Su tecnología fue utilizada para reprimir las revoluciones árabes, a través de un sistema de vigilancia vinculado con la red de telecomunicaciones por el régimen de Al-Assad en **Siria**[50], así como por el régimen de Ben Ali en **Túnez**[51]. En el caso de Siria, Utimaco cooperó también con las empresas italiana Area SpA y la francesa Qosmos SA.

48 **Total Secure Defence.** "IMSI Catchers and Interception Systems in Morocco," Total Secure Defence. Disponible en: https://totalsecuredefence.com/imsi-catchers-and-interception-systems-morocco/

49 **Trevor Timm.** "Spy Tech Companies and Their Authoritarian Customers, Part II: Trovicor and Area Spa," Electronic Frontier Foundation, 21 de febrero de 2012. Disponible en: https://www.eff.org/deeplinks/2012/02/spy-tech-companies-their-authoritarian-customers-part-ii-trovicor-and-area-spa

50 **Der Spiegel.** "Is Syrian monitoring protesters with German technology?" 2011. Disponible en: https://www.spiegel.de/international/world/police-state-is-syria-monitoring-protesters-with-german-technology-a-796510.html

51 **Privacy International.** "State surveillance in Tunisia." 2019. Disponible en: https://www.privacyinternational.org/state-privacy/1012/state-surveillance-tunisia

- **URS:** empresa norteamericana fundada en 1951 y especializada en servicios técnicos de ingeniería y construcción. En 2014, la también norteamericana AECOM se hace con su control. URS aporta, en 2018, sistemas de cámaras de videovigilancia modernas con alta resolución, largo alcance, detección térmica y de movimiento al muro fronterizo entre **Túnez**[52] y **Libia**[53].
- **VASTech:** empresa con sede en Sudáfrica que en asociación con AGT, ha suministrado diversas tecnologías de interceptación de las comunicaciones en **Siria**[54].
- **Veridos:** empresa con sede en Berlín que surge de la fusión, en 2014, de dos empresas alemanas líderes en el sector de la tecnología de seguridad e identidad digital Giesecke+Devrient y Bundesdruckerei. En 2016 inician la implementación de un sistema de reconocimiento biométrico para el control de fronteras en **Marruecos**[55].

52 **Kapitalis.** "Des Américains installent la surveillance électronique au sud de la Tunisie," 14 de agosto de 2016. Disponible en: https://kapitalis.com/tunisie/2016/08/14/des-americains-installent-la-surveillance-electronique-au-sud-de-la-tunisie.

53 **Africa Intelligence.** "Washington Consolidates Tunisia-Libya Electronic Border Surveillance Wall," 12 de febrero de 2021. Disponible en: https://www.africaintelligence.com/north-africa/2021/02/12/washington-consolidates-tunisia-libya-electronic-border-surveillance-wall,109642877-art

54 **Privacy International.** "Open Season: The Global Surveillance Industry," Diciembre 2017. Disponible en: https://privacyinternational.org/sites/default/files/2017-12/OpenSeason_0.pdf.

55 **Veridos.** "Morocco & the U.S.: Secure ID Solutions," Veridos. Marzo 2020. Disponible en: https://www.veridos.com/files/assets/downloads/pdf/Flyer_Morocco_US_A4_03-2020_Download.pdf